CLIN 001 - AUDIT SUPPORT SERVICES

1. OVERVIEW

The Security Governance Branch, within the Security Division, is responsible for policies, controls and plans which ensure that risks are managed appropriately. The branch provides strategic direction, ensures that objectives are achieved, and verifies that the enterprise's resources are used responsibly and are consistent with applicable Federal laws and regulations. The Branch is made up of three teams: Contingency Planning, Risk Management, and Internal Audit.

The objective is to obtain technical support for two of the Internal Audit Team's (IAT) missions: (1) performing the continuous assessment tasks of the USDA's Continuous Assessment and Authorization (A&A) process of the USDA Six Step Risk Management Framework (RMF) Process[1], and (2) annual A-123 testing. The contractor may be required to make contacts with NITC customers, technical staff, business partners, managers, and internal and external auditors.

2. SCOPE/DUTIES

a) The scope covers the systems listed in the NITC Systems table below.

System Name	Acronym	System Type	Assessment Type
NITC Enterprise Services	ES	General Support System	Cont. Assess. A-123
NITC Auxiliary Support System	AXS	General Support System	Cont. Assess. A-123
NITC Customer Billing System	CIMS	Major Application	Cont. Assess. A-123
NITC Data Center	NITC Data Center	Site	Cont. Assess. A-123
NITC Facility Security System (On Guard)	OnGuard	Major Application	Cont. Assess.
NITC Internal Services	NIS	Site	Cont. Assess. A-123
NITC ITSM Services Environment	ISE	Major Application	Cont. Assess.
NITC Mainframe	NITC Mainframe	General Support System	Cont. Assess. A-123
NITC Management Support System	MSS	Minor Application	Cont. Assess.
NITC Midrange Systems	NITC Midrange	General Support System	Cont. Assess. A-123
NITC Telecommunications Network GSS	NITC Network	General Support System	Cont. Assess. A-123
NITC Web Farm Hosting	NITCWebFarm	General Support System	Cont. Assess. A-123

b) For the systems listed as "Cont. Assess." (Continuous Assessment), the contractor shall perform the continuous assessment tasks of continuous assessment and authorization (A&A) process (Step 4 of the RMF process) according to Appendix E - Security Controls Assessment List. The A&A process requires annual testing of approximately one-third of the controls with 100% of the controls tested within a three year cycle. These tasks include, but are not limited to:

i. Develop and document the Test Plan.
ii. Execute accepted test plan and assess the Security Controls.
iii. Develop security assessment reports and recommend Plans of Action and Milestones (POA&M).

[1] USDA Six Step Risk Management Framework Process (RMF) Guide

iv. Upon completion of the above tasks (identified as i, ii and iii), manage the process of completing the Step 4 Concurrency Review.

c) For the systems listed in the NITC Systems Table as "Cont. Assess. A-123", the contractor shall perform the A-123 assessment of the NITC systems according to the guidance provided by the USDA Office of Chief Financial Officer (OCFO) Senior Assessment Team (SAT). The tasks to be completed, according to OCFO SAT guidelines, include:
   i. Develop and document the Test Plan.
   ii. Execute General Computer Controls (GCC) testing in accordance with accepted test plan.
   iii. Document Testing Results in Cyber Security Assessment Manager (CSAM).
   iv. Develop the following reports and documentation: security assessment reports; Corrective Action Plans (CAPs) with recommendations, and the Summary of Aggregated Deficiencies (SAD).
   v. Recommend Plans of Action and Milestones (POA&Ms).
   vi. Draft Annual Certification Statements.
d) The contractor shall update assessments when revisions to National Institute of Standards and Technology Special Publication (NIST SP) 800-53, and other applicable regulations and guidance, are adopted by the agency.
e) Develop and execute a project plan(s) that defines responsibilities, timelines, deliverables, risks, and milestones necessary to accomplish the stated objectives.
f) Provide a weekly project status report, orally and in writing.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Working knowledge of the technical requirements of applying the Risk Management Framework to Federal information systems in an enterprise Federal data center.
b) Working knowledge of the technical requirements of performing OMB Circular No. A-123 assessments to Federal information systems in a large Federal data center.
c) Working knowledge of the technical requirements of applying the Federal Risk and Authorization Management Program (FedRAMP) requirements to Federal information systems in a large Federal data center.
d) Proficient using MS-Word, MS-Excel and MS-Project software, and possess strong abilities in writing technical documents. Skilled in facilitating meetings.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Continuous Assessment Tasks	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant all with applicable governing regulations, policies, directives and guidance. ▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
A-123	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant all with applicable governing regulations, policies, directives and guidance. ▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Project Planning and Management	▪ The contractor shall develop, document, and maintain project plans 100% compliant with federal governing regulations, policies, directives, guidance and industry practice. ▪ 100% of project plans shall include the identification of applicable responsibilities, timelines, deliverables, risks, milestones and other elements as required. ▪ 100% of plan schedules and activities shall be coordinated with all required participants. ▪ All issues impacting project schedules shall be communicated to government staff within one business day after determination of impact. ▪ 100% of project plans shall be updated weekly.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Weekly Status Report	▪ 100% complete. ▪ 100% accurate. ▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period.	▪ No more than 1 violation per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

CLIN 002 - BUDGET ANALYSIS SUPPORT SERVICES

1. OVERVIEW

The contractor shall provide budget analysis support to the Budget Management Branch at NITC. Budget Analysis assignments may be internally focused within the branch or in support of an initiative coming from a customer or other organizational unit. Budget analysis services enable effective coordination and utilization of all other support services by planning and review of program execution with a goal of providing value to NITC customers for services received.

2. SCOPE/DUTIES

a) The contractor shall support budget analysis tasks that include monitoring budget reservations and executions, initiating execution of accounting transactions, analyzing and reconciling transactions with budget plans, and assuring compliance with regulations, directives, procedures, and guidelines.
b) The contractor shall prepare and maintain business-line level spend plans and track funds reservations and execution by Standard General Ledger (SGL) account.
c) The contractor shall support internally focused requirements/tasks and provide deliverables, which may include, but are not limited to, the following: reconciliation of accounts and income; assisting with analysis of reports, completion of documentation; preparation of document packages for audit review; and analysis of budget data. The contractor may be assigned to either a single or multiple NITC business lines, which may consist of between 400 and 600 budget line items.
d) The contractor shall prepare, submit, and maintain BOC Rollup Summary reports identifying planned requirements, SGL account execution, and expected rest-of-year requirements broken down by Mandatory, Center Capacity, and Discretionary. Additional breakdowns showing current-month and rest-of-year amounts may be required. The BOC Rollup Summary shall also include a version-over-version explanation of changes to spend plan amounts by BOC Rollup. The BOC Rollup Summary reports shall be delivered at specified mid-month and end-of-month management briefing dates.
e) The contractor shall prepare, submit, and maintain monthly Working Capital Fund (WCF) operating plan versus actual variance reporting results and explanations for current fiscal years using the required WCF tool & NITC format. The reporting results and related information shall be delivered no later than the Thursday immediately preceding the monthly WCF Status of Funds (SoF) reporting deadline (typically the 15th of each month).
f) The contractor shall prepare, submit and maintain monthly support services plan / actual usage reconciliation report with full-year trend analysis. The report shall be delivered at the mid-month management briefing.
g) The contractor shall support externally focused requirements/tasks and provide deliverables, which may include, but is not limited to, providing other branches, offices, or agencies with budget data and analysis.

h) Both types of support and deliverables (internally focused and externally focused) will require synthesis and presentation of data, development of alternative courses of action, and recommendations to decision makers.
i) Increased requirements associated with end-of-year financial activities will likely result in the need for the contractor to provide support that extends beyond a typical/standard work week (i.e. 40 hours) during the month of September. Requirements may increase by approximately 25% during this timeframe. The contractor shall fully support such requirements.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Advanced Microsoft Office Excel skills.
b) Working knowledge of General Accepting Accounting Principles (GAAP).
c) Problem solving and analysis skills.
d) Government accounting experience is preferred.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Spend Plans and Tasks	▪ 100% of spend plan documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.). ▪ 100% of spend plan documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input
BOC Deliverables and Tasks	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents. ▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input
WCF Deliverables and Tasks	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents. ▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input

Usage Reconciliation Deliverables and Tasks	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents. ▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input
Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input
Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

CLIN 003 - BUSINESS CONTINUITY PLANNING SERVICES

1. OVERVIEW

The Security Governance Branch, within the Security Division, is responsible for policies, controls and plans which ensure that risks are managed appropriately. The branch provides strategic direction, ensures that objectives are achieved, and verifies that the enterprises' resources are used responsibly and are consistent with applicable Federal laws and regulations. The Branch is made up of three teams: Contingency Planning, Risk Management, and Internal Audit.

The objective is to obtain services to support the NITC Business Continuity Program. The contractor shall develop IT disaster recovery (DR) and continuity of operations (COOP) plans and test schedules and shall coordinate and conduct COOP and DR tests.

The contractor may be required to make contact with NITC customers, technical staff, business partners, managers, and internal and external auditors.

2. SCOPE/DUTIES

a) The contractor shall work closely with the NITC Security Staff Contingency Management team and support the creation and maintenance of detailed DR plans for NITC IT systems, services and platforms in accordance with all applicable standards as identified by NITC, OCIO and applicable federal laws, regulations, policies and guidance.
b) Conduct planning meetings with technical systems personnel to gather requirements and data required for the creation and documentation of IT DR plans for the Enterprise Data Center.
c) Develop test schedules and plans, and support exercises for ITDR tests and call tree tests. Typically the NITC performs the following exercises:
    i. Annually:
        - Four (4) notification (call tree) exercises.
        - Two (2) functional exercises.
        - Two (2) tabletop exercises.
    ii. Monthly:
        - One (1) tabletop exercise.
        - Customer validation exercises, as required.
d) Coordinate and track remedial actions, as necessary, following tests, training and exercises and create after action reports for presentation to NITC management by NITC staff.
e) Perform business impact analysis for assigned IT systems, services or platforms. This includes the following:
    i. Develop survey questions.
    ii. Analyze documentation and/or survey results to ascertain which system, service or platform supports a mission critical business process.

iii. Develop and present achievable recovery time objectives (RTO) and recovery point objectives (RPO) as it relates to internal or customer IT systems, services or platforms.
iv. Develop and propose DR strategies and plans stemming from analysis of documentation, surveys and discussions with subject matter experts (SME).

f) Participate in special initiatives or projects where contingency planning or DR expertise is required. For example, assist in the planning and implementation of new DR strategies or processes. Assist in the publication and distribution of contingency planning documents.
g) Develop and maintain COOP and DR documentation as it pertains to the accreditation of IT systems, services or platforms.
h) Develop, maintain and deliver presentations regarding COOP and DR practices which include classroom training, workshops and formal or informal briefings to technical and senior NITC staff. Presentations and documents shall be developed using standard office automation tools such as Microsoft Office, Project and Visio.
i) Provide routine technical knowledge transfer to identified NITC technical staff.
j) Actively participate in meetings or discussions to provide status and resolve issues related to assigned IT systems, services or platforms.
k) Perform analysis of security tasks to identify areas where there may be overlapping or redundant tasks which can be optimized or modified to create efficiencies or economies of scale on assigned IT systems, services or platforms.
l) Respond to customer inquiries via email or telephone, from both internal and external customers, with timely, accurate information, within 24 hours.
m) Maintain DR data in the LDRPS database.
n) Maintain Call Tree data in the MIR3 system.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Well versed in the technical areas of disaster recovery planning and business resumption planning for information technology operations.
b) Expert level experience in developing and maintaining IT Disaster Recovery (ITDR) Plans, coordinating ITDR exercises, developing ITDR test and exercise plans, auditing tests and exercises in order to determine weaknesses, strengths, and remedial actions required to ensure effective recovery capabilities for a large Federal data center, and preparing after action assessments, reports and lessons learned.
c) Experience in developing and conducting business impact assessments (BIA), analyzing results of BIAs and coordinating with technical teams to develop recovery solutions based on BIA results.
d) Experience conducting and assessing emergency alert and notification drills, documenting test, training and exercise plans and after action reports.
e) Experience developing or maintaining Business Continuity Plans, Continuity of Operations Plans, and Crisis Communications Plans. This includes interviewing subject matter personnel to ascertain the mandatory elements of various types of contingency plans.

f) Experience in preparing and giving disaster recovery and emergency response presentations for customers.
g) Sound knowledge of Federal directives regarding continuity of government and continuity of operations requirements or a sound knowledge of national standards for disaster or emergency management and business continuity programs for private industry.
h) Experience providing advice and assistance in the following: developing overall continuity of operations strategies, emergency response, team deployment, employee and family assistance for trauma, human capital planning for emergencies, emergency operations, guidelines for determining and operating at alternate facilities, and incident management.
i) Proficient using MS-Word, MS-Excel and MS-Project software, and possess strong abilities in writing technical documents. The contractor must have experience in facilitating meetings.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
DR and COOP Plans and Tasks.	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant with applicable governing regulations, policies, directives and guidance. ▪ 100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

DR and COOP Test Documentation and Tasks.	▪ 100% of documentation is prepared via the utilization of required tools as applicable. ▪ 100% of test schedules, methods, and activities shall be coordinated with all required participants and submitted NLT the established date for completion/receipt as identified in the requirement documents. ▪ 100% of participants shall have access as required to successfully participate in test activities. ▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant with applicable governing regulations, policies, directives and guidance. ▪ 100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Weekly Status Report	▪ 100% complete. ▪ 100% accurate. ▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period.	▪ No more than 1 violation per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

CLIN 004 - ENTERPRISE INFORMATION TECHNOLOGY SERVICES PORTFOLIO MANAGEMENT

1. OVERVIEW

The Service Portfolio Branch manages the portfolio suite of technology services, and accompanying business processes that enable the United States Department of Agriculture (USDA) to achieve its goals and objectives of eGovernment, leveraging its investments and delivering government services in a more citizen-centric manner.

The services offered by the National Information Technology Center (NITC) Enterprise Data Center (EDC) are enterprise-wide. Department, Agency, or Federal eGovernment initiatives can leverage these services. USDA Agencies and initiatives do not have to create their own technology solutions and standards and can instead utilize the NITC EDC centralized service offerings to support their business requirements and thus avoid the high cost and high learning curve of operating these solutions independently.

2. SCOPE/DUTIES

a) Services Architecture. The contractor shall support tasks including, but not limited to, the following:
   i. Participate in identifying and prioritizing the next steps for the technical environments. As agency use increases, components of the architecture are upgraded, and new requirements surface, changes to the service offering may be necessary to assure that the technical environments, the application support as well as the financial impact are fair, equitable and functioning as expected. Any deviations from these service scopes will need to be identified as early as possible, planned and tracked to implementation.
   ii. Identify and managing new services offerings from cradle to grave.
   iii. Plan support of and integration with any new service offerings, such as collaboration or records management. This includes discussions with NITC technical teams to determine the necessary steps to support new offerings such as identifying hardware and software components as well as identifying customized code that might be necessary to support the service in the existing architecture.
   iv. Develop technical standards for all environments. These standards should follow best practices and support the NITC EDC architecture.

b) Agency Liaison / Software Consulting. The contractor shall support tasks including, but not limited to, the following:
   i. Facilitate agency meetings and workshops. As agencies express interest in the use of the NITC EDC service offerings and want to develop applications in this framework, a pre-implementation meeting will occur between agency teams and the NITC Account Manager, with support from the Agency Liaison. Workshops may be scheduled to expedite agency planning and implementation of requirements. This support involves meeting logistics, preparation of materials, and planning work prior to and after the meeting to correctly guide the agency through the processes of transitioning to NITC EDC services. Additionally, the Agency Liaison

shall provide support with technical details and information about the architectures of NITC EDC services.

ii. Agency Adoption Support. Agency Liaisons and their government NITC EDC Business Development counterpart will work directly with agencies to support their use of NITC EDC services. This support will include initial discussion of the tools and their abilities, coordination of tool access, and communication with data center and operations entities. In the longer term, this support will include a marketing aspect as well as communicate to the agencies the proper use of the tools and the services.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Experience with overall enterprise data center services life cycle development as well as the development and maintenance of service catalogs, in support of the organizational mission.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Product Management Analysis Deliverables and Tasks	▪ 100% of applicable service offerings shall be analyzed and reported within the applicable annual period. ▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.), to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.	▪ No more than 4 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Portfolio Services Deployment Deliverables and Tasks	▪ 100% of on-going documentation and reporting of NITC Service Development milestone achievements shall be provided for new services proposed from the NITC Service Development Portal as defined by the NITC Service Development Lifecycle Directive. ▪ 100% attendance and active participation in all facilitation/collaboration/consultation events as required. ▪ 100% of facilitation/collaboration/consultation presentations and communications shall be coordinated as required and shall be clear, effective, concise, and organized. ▪ 100% of facilitation/collaboration/consultation activities shall be tailored specifically for subject matter needs and shall result in the team's ability and empowerment to achieve documented action items and milestones. ▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.	▪ No more than 4 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery. ▪ Facilitation ineffectiveness may be determined to be a violation.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Documentation	▪ 100% of all NITC Service Catalog documentation shall be produced and maintained, including the performance and documentation of required modifications/adds/deletes, to ensure accurate representation of NITC Service offerings. ▪ 100% of all NITC Services Appendices documentation shall be produced, edited, reviewed, distributed and maintained, including the performance and documentation of required modifications/adds/deletes, to ensure accurate representation of NITC Service offerings. ▪ 100% of documentation shall be updated IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance. ▪ Electronic versions of all documentation in the required format shall be posted/stored in the required artifact repository/tool location within the mutually established timeframe and shall be available for Government review at all times as required.	▪ No more than 4 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Weekly Status Report	▪ 100% complete. ▪ 100% accurate. ▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period.	▪ No more than 1 violation per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 4 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

CLIN 005 - FACILITIES OPERATIONS SERVICES

1. OVERVIEW

The objective of this CLIN is to obtain technical support services for the National Information Technology Center (NITC) Data Center in support of the Service Portfolio Branch. The contractor shall serve as a Facilities Operations Specialist responsible for project management activities in support of data center mission capabilities, including change, problem and inventory management. The contractor shall support the overall operation of the data center and oversees data center facilities plans and proposals as well as ensuring all security requirements are met in accordance with Government guidelines and standards. The contractor shall assist in and support increasing program effectiveness by evaluating current facility operation services and assisting in the development of new services. This position may require making contacts with NITC customers, technical staff, business partners, management, and internal/external auditors.

2. SCOPE/DUTIES

a) Plans and develops electrical power needs for new and existing equipment in the Centers by applying a thorough and practical knowledge of engineering methods and techniques. Takes into account characteristics of electrical power systems to draft, design, analyze and review plans for power distribution, ground grid systems, electrical circuitry, size of conduit, wire, etc., necessary for installing Center support systems. Translates plans into specification tasks as required. The contractor shall assist the NITC facilities manager as required, to include the updating of existing documentation or creation of new documentation using Microsoft Office products, and AutoCAD.
b) Monitoring of office and computer room environmental conditions such as air conditioning, heat, power, generators, and air plenum to ensure computer system availability as required. Identifies and analyzes potential problems and prepares alternative solution for consideration. The contractor shall follow procedures and instructions to specify method of repair, modification, maintenance and testing of environmental systems.
c) Identifies electrical, space, and cooling requirements for new IT hardware. Monitors environmental controls to ensure the computer room is operating at peak performance at all times. Physically assists when needed to support the installation of hardware in rack space on the data center floor; setting up conference rooms; assisting with day to day facility operations; documenting equipment installation, configuration, and electrical connection; and distribution of applicable documentation to asset management personnel as required.
d) Perform quality assurance activities in support of maintenance operations.
e) Submit recommendations and justifications to modernize or improve structures and equipment. Provides input into performance profile surveys, equipment inspections, technical troubleshooting, maintenance evaluations, and workload analysis.
f) Review, analyze and evaluate deficiency reports and equipment malfunction reports. Considers significance of failures in regard to safety hazards, cost of repairs, loss or downtime of equipment, and delays resulting from lack of available parts.

g) Evaluate and determine the quality and quantity of repair parts and tools to reduce unnecessary duplication and variety, as well as to ensure that needed materials are on hand.
h) Perform preparation and restoral activities associated with the installation and removal of equipment related to work areas consisting of heating, ventilating, air conditioning, high/low voltage electrical, carpentry, painting, masonry, sheet metal work and similar trades. Prepare inspection reports for the purpose of identifying and recommending solutions to problems involving lack of personnel, materials, poor workmanship, conditions in need of repair, and various other related concerns.
i) Responsible for facilities related hardware systems ingress and egress from the data center floor. Receives and installs hardware from agencies or vendors. Determine power requirements and coordinate electrical service installation for hardware. Support the procurement and complete the installation of low voltage cabling to provide connectivity to existing systems and to internal KVM monitoring systems.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Overall project management of secure data center facilities projects, including projects related to the infrastructure systems and equipment of the center.
b) Experience with the management of mechanical, electrical, and environmental requirements associated with a computer room environment.
c) Working knowledge of computer protection devices and environmental systems, including, but not limited to, the following: uninterruptible power systems, diesel generators, transfer switches, paralleling gear, computer room air-conditioning, security, and fire protection systems.

1. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Facility Technology Analysis Deliverables and Tasks	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.), to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.	▪ No more than 2 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input
Design and Implementation Planning Deliverables and Tasks	▪ 100% of documentation shall be clear, concise, organized and developed with required tools as applicable. ▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.	▪ No more than 2 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input

Documentation Updates and Storage/Repository	▪ 100% of documentation shall be updated IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance. ▪ Electronic versions of all documentation in the required format shall be posted/stored within the mutually established timeframe in the required artifact repository/tool location and shall be available for Government review at all times as required.	▪ No more than 2 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input
Weekly Status Report	▪ 100% complete. ▪ 100% accurate. ▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period.	▪ No more than 1 violation per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $1,500.00.	Checklist and Customer Input
Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 2 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input

Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

.

CLIN 006 - INFORMATION SYSTEMS SECURITY SUPPORT SERVICES

1. OVERVIEW

The Security Governance Branch, within the Security Division, is responsible for policies, controls and plans which ensure that risks are managed appropriately. The branch provides strategic direction, ensures that objectives are achieved, and verifies that the enterprises' resources are used responsibly and are consistent with applicable Federal laws and regulations. The Branch is made up of three teams: Contingency Planning, Risk Management, and Internal Audit.

The objective is to obtain technical support for the Risk Management Team's (RMT) mission of performing the continuous authorization tasks of the USDA's Continuous Assessment and Authorization (A&A) process of the USDA Six Step Risk Management Framework (RMF) Process (USDA Six Step Risk Management Framework Process (RMF) Guide). The contractor may be required to make contact with NITC customers, technical staff, business partners, managers, and internal and external auditors.

2. SCOPE/DUTIES

a) The scope covers the systems listed in the NITC Systems table below.

System Name	Acronym	System Type	Assessment Type
NITC Enterprise Services	ES	General Support System	Cont. Assess. A-123
NITC Auxiliary Support System	AXS	General Support System	Cont. Assess. A-123
NITC Customer Billing System	CIMS	Major Application	Cont. Assess. A-123
NITC Data Center	NITC Data Center	Site	Cont. Assess. A-123
NITC Facility Security System (On Guard)	OnGuard	Major Application	Cont. Assess.
NITC Internal Services	NIS	Site	Cont. Assess. A-123
NITC ITSM Services Environment	ISE	Major Application	Cont. Assess.
NITC Mainframe	NITC Mainframe	General Support System	Cont. Assess. A-123
NITC Management Support System	MSS	Minor Application	Cont. Assess.
NITC Midrange Systems	NITC Midrange	General Support System	Cont. Assess. A-123
NITC Telecommunications Network GSS	NITC Network	General Support System	Cont. Assess. A-123
NITC Web Farm Hosting	NITCWebFarm	General Support System	Cont. Assess. A-123

b) For the systems listed as "Cont. Assess." (Continuous Assessment), the contractor shall perform the continuous authorization tasks of continuous assessment and authorization (A&A) process (Steps 1-3 of the RMF process) according to Appendix E - Security Controls Assessment List.

c) The contractor shall review and update the system security plan, including one third of the controls, annually and the entire system at least every three years.
   i. Review and update the system security plan.
      - The Mission/Purpose
      - The Information Types
      - The Locations
      - The Interconnections

- The System Description and Technical Description Narratives
- The Points of Contact.
- The appendices:
  - K2 - MOU/SLA Agreements
  - O - Incident Response Plan
  - Q2 - Configuration Management Plan
  - R - Accreditation Statement and Documentation
  - S - Hardware Listing
  - T - Software Listing
  - V2 - Privacy Threshold Analysis
  - V3 - Privacy Impact Assessment

ii. Working with control owners, review and update the appropriate control Implementation Statements, according to Appendix E - Security Controls Assessment List. This constitutes about one-third of the controls that apply to the system.

iii. Upon completion of the above tasks (identified as i and ii), manage the process of completing the Step 3 Concurrency Review.

d) The contractor shall update control sets when revisions to National Institute of Standards and Technology Special Publication (NIST SP) 800-53, and other applicable regulations and guidance, are adopted by the agency.

e) Develop and execute a project plan(s) that defines responsibilities, timelines, deliverables, risks, and milestones necessary to accomplish the objectives of the task.

f) Provide a weekly project status report, orally and in writing.

3. EXPERIENCE REQUIRED

a) Working knowledge of the technical requirements of applying the Risk Management Framework to Federal information systems in an enterprise Federal data center.

b) Working knowledge of the technical requirements of applying the Federal Risk and Authorization Management Program (FedRAMP) requirements to Federal information systems in a large Federal data center.

c) Proficient using MS-Word, MS-Excel and MS-Project software, and possess strong abilities in writing technical documents. Skilled in facilitating meetings.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Security Plans and Tasks	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant all with applicable governing regulations, policies, directives and guidance. ▪ 100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery. ▪ No more than 10 findings resulting from the first round of the Step 3 Concurrency Review, and those findings are corrected within 5 business days.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Implementation Statements and Tasks	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant all with applicable governing regulations, policies, directives and guidance. ▪ 100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Project Planning and Management (including Step 3 Concurrency Review)	▪ The contractor shall develop, document, and maintain project plans 100% compliant with federal governing regulations, policies, directives, guidance and industry practice. ▪ 100% of project plans shall include the identification of applicable responsibilities, timelines, deliverables, risks, milestones and other elements as required. ▪ 100% of plan schedules and activities shall be coordinated with all required participants. ▪ All issues impacting project schedules shall be communicated to government staff within one business day after determination of impact. ▪ 100% of project plans shall be updated weekly. ▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.). ▪ 100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Weekly Status Report	▪ 100% complete. ▪ 100% accurate. ▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period.	▪ No more than 1 violation per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

CLIN 007 - INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM) PROCESS DEVELOPMENT AND DOCUMENTATION SERVICES

1. OVERVIEW

The objective is to obtain Information Technology Service Management (ITSM) process development and documentation support for the National Information Technology Center (NITC), Infrastructure Operations Division, IT Service Management Branch (IOD/ITSMB). This position may require making contacts with NITC customers, technical staff, business partners, management, and internal/external auditors.

2. SCOPE/DUTIES

a) Perform process gap analysis, monitor and assess defined key performance indicator (KPI) and metrics.
b) Develop and manage the software development lifecycle artifacts including Business, Functional and Technical Requirements, Functional Design Documents, Use Cases, Process Models, Data Flow Diagrams, etc., as required.
c) Develop software and technology requirement specification documents, as required. Liaise with the Service Transition Process Owners, Process Managers, NITC IT and Business Staff throughout Process Analysis, Design, Development, Testing and Implementation for Service Transition process improvements.
d) Create, facilitate and develop end user acceptance testing plans according to the documented business, functional and technical requirements and process design documents necessary to meet business process and technology requirements.
e) Provide end user process training materials, as required.
f) Plan and coordinate new service design packages through the Service Transition model, as required.
g) Create, test and release, change request templates and task templates for Service Request Fulfillment and Change Management process and technology requirements.
h) Create IT Service Transition procedures and processes as required.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Expert-level analytical and problem-solving skills.
b) Certified in ITIL Foundations v3.
c) Ability to manage multiple requirements simultaneously
d) Experience with ITSM technical writing.
e) Proficiency in MS Office products.
f) BMC Remedy Enterprise Suite experience.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
ITSM Process Development and Documentation Services Task/Product Activities	▪ 100% of all ITSM Process and Development and Documentation activities shall be conducted in accordance with governmental & organizational standards, policies, directives, standard operating procedures, work instructions, processes & guidance. All operational support activities shall be captured and properly documented in the organizational ITSM tool. The contractor shall adhere to this requirement unless a written exemption is issued by an authorized Government representative.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $10,000.00.	Checklist and Customer Input
Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

CLIN 008 - INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM) SERVICE ASSET AND CONFIGURATION MANAGEMENT SUPPORT SERVICES

1. OVERVIEW

The contractor shall provide Service Asset and Configuration Management support across the various organizational units at the National Information Technology Center (NITC). Service Asset and Configuration Management coordination, within the current environment, may require the contractor to provide direct support to NITC customers, technical staff, management, and internal and external auditors.

The contractor shall perform in a Service Asset and Configuration Management specialist capacity supporting the maintenance, administration, quality and accuracy of the NITC Service Asset and Configuration Management centralized data repository, Configuration Management Database (CMDB) through the asset management applications.

2. SCOPE/DUTIES

The Government will issue contractor task assignments via the organization ITSM suite.

a) The contractor shall support internally focused requirements/tasks and provide deliverables, which may include, but are not limited to, the following: managing Atrium CMDB Configuration Item (CI) updates along with other associated asset information, data analysis, auditing and reporting, measure performance and data quality, and administration of the Atrium Core console functions such as automated or manual data normalization and reconciliation.
   i. Atrium CMDB Updates
      - Perform assigned end user requested CI quality updates via incident service request tickets and approved change records.
      - Perform automatically assigned CI update tasks from within submitted and approved change records.
      - Perform assigned product catalog and Definitive Media Library (DML) item updates via submitted and approved change records.
      - Perform assigned end user requested inventory location updates via incident service request tickets and approved change records.
      - Perform end user requested customer project updates including the changing of CIs related to projects via submitted and assigned incident service request tickets and approved change records.
      - Perform end user requested master contract updates including the changing of CIs related to contracts via submitted and assigned incident service request tickets and approved change records.
      - Perform technical or business service CI updates for Atrium Discovery and Dependency Mapping (ADDM) application to service discovered CIs via submitted and approved change records.
   ii. Atrium CMDB Reporting

- Perform scheduled queries, exports and reports of CI or other CMDB related data by the defined format and store within designated file locations. Scheduled queries, exports and reports include, but are not limited to:
  - Full Hardware CI Export
  - Full Dataset Export (all datasets configured)
  - CIs Created in past 30 days
  - CIs Decommissioned in past 30 days
  - CIs disposed in past 30 days
  - CIs received in past 30 days
  - Percentage and count of CIs discovered by ADDM (scanning and discovery tool)
  - Percentage and count of CIs not discovered by ADDM (scanning and discovery tool)
  - Percentage and count of CIs with incomplete, required attributes
  - Percentage and count of Unauthorized CIs (created or updated without a change record)
  - Percentage and count of CIs unidentified or identified incorrectly by platform service, service role, service rate, project and customer agreement
- Perform assigned end user requested ad-hoc CI exports or reports via incident service request tickets.
- Update Standard Operating Procedures (SOPs) that are affected by government changed Service Asset and Configuration Management policies, process or CI or other related data specifications.

iii. Atrium CMDB Administration
- Run and monitor manual atrium reconciliation and normalization jobs and resolve errors according to defined procedures.
- Perform manual atrium identification on all reconciliation jobs and resolve conflicts or errors according to defined procedures.
- Identify and verify IT infrastructure configuration items such network, security, hardware and software assets and the relationships between them.

b) The contractor shall support externally focused requirements/tasks and provide deliverables which may include, but are not limited to, providing other branches, offices, or agencies with asset data and analysis. Both types of deliverables will require presentation of data, development of alternative courses of action, and recommendations to decision makers.

c) The contractor shall implement and employ Service Asset and Configuration Management IT Infrastructure Library (ITIL) processes and principles that are aligned with NITC approved policy.

d) The contractor shall provide weekly status reporting to the Alternate Contracting Officer's Representative – Technical (ACORT).

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) BMC Atrium CMDB.
b) BMC ITSM suite.

c) Well developed personal computing skills and knowledge of standard MS Office Products, such as Outlook, Excel and Word. The ability to generate accurate ADHOC reports using these programs is required.
d) Teamwork, coordination, analytical thinking, problem-solving, and documentation are critical aspects of success in performing the required tasks.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
ITSM Service Asset and Configuration Management Task/Product Activities	▪ 100% of all ITSM Service Asset and Configuration Management activities shall be conducted in accordance with governmental & organizational standards, policies, directives, standard operating procedures, work instructions, processes & guidance. All operational support activities shall be captured and properly documented in the organizational ITSM tool. The contractor shall adhere to this requirement unless a written exemption is issued by an authorized Government representative.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $10,000.00.	Checklist and Customer Input
Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

PROGRAM/PROJECT MANAGEMENT SUPPORT SERVICES

1. OVERVIEW

The contractor shall provide project management support across the various organizational units at the National Information Technology Center (NITC). Project management assignments may be internally focused or in direct support of a customer initiative. Internally focused projects may include infrastructure upgrades, software version upgrades, security implementations, and development of new service offerings. Externally focused projects may include customer business application migrations from one data center hosting platform to another, customer disaster recovery support, and customer business application migration to the data center from an external hosting provider. The Government will issue written project assignments to the contractor. The contractor shall implement and employ project management methodologies that are aligned with NITC approved policy.

Project Management coordination, within the current environment, may require contractor staff to provide direct support to NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

a) General Tasks. General tasks include, but are not limited to, the following: managing internal and external projects utilizing the tools and methodology defined by the NITC Project Management Office (PMO); refining, enhancing, and improving the NITC PMO toolset, methodology, and practices; knowledge transfer and informal training; reporting status to Alternate Contracting Officer's Representative – Technical (ACORT); management of a project's critical path; and facilitating organization change towards a more project management oriented culture. Teamwork, coordination, and documentation are critical aspects of success in performing the tasks.

b) Initiating Phase. The contractor shall perform processes to define a new project or new phase of an existing project by completing work to establish the project charter and gain Government/stakeholder acceptance. Depending on projected cost of the project, the initiation phase may be governed by the Office of the Chief Information Officer's (OCIO's) Capital Planning and Investment Control thresholds. Tasks include, but are not limited to, the following: documenting objectives, developing a project charter, identifying a project sponsor and stakeholders, defining high level deliverables, projecting deliverable completion dates, identifying resource requirements, and gaining Government approval. Required templates include: Project Charter, Project Weekly Status Report and/or Minor Project Weekly Status Report.

c) Planning Phase. The contractor shall perform processes to identify the tasks and work assignments to complete an approved project charter. Tasks include, but are not limited to, the following: estimating schedules, sequencing tasks, documenting risks, developing risk mitigation strategies, documenting project alternatives/assumptions/constraints. Required templates include: Work Breakdown Structure, Risk Matrix, and Project Weekly Status Report.

d) Executing Phase. The contractor shall perform activities such as project team facilitation, project team solution generation, project team coaching for breakthrough performance, project management plan monitoring, project deliverable tracking, and management reporting. The contractor shall possess "people skills" to gain the confidence, trust and respect throughout the organization while ensuring that project team members are treated with dignity and respect. Through the project monitoring activities, the contractor shall ensure that the work breakdown structure correctly identifies the critical path tasks/work activities within one (1) business day of identifying a deviation. Required templates include: Work Breakdown Structure, Critical Path Diagram, and Project Weekly Status Report.
e) Controlling Phase. The contractor shall perform analysis activities to compare actual performance with planned performance, identify and report variances, evaluate possible migration strategies, perform earned value management (when required), recommend appropriate corrective actions, and communicate to seek guidance from the Project Sponsor (Stakeholders), as applicable.
f) Close Out Phase. The contractor shall perform activities to assemble project artifacts in a historical repository. Tasks include, but are not limited to, the following: formalizing customer acceptance, preparing a final project performance report, documenting lessons learned, and archiving project records.
g) The contractor shall support all meeting and reporting requirements.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Project Management Professional (PMP) certification.
b) Experience with Government EVM requirements is preferred.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Project Planning and Management Deliverables and Tasks	▪ 100% adherence to mutually agreed upon project management tasks, activities, and objects/artifacts established and documented in the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.). ▪ The contractor shall develop, document, and maintain project plans 100% compliant with federal governing regulations, directives, guidance and industry practice. ▪ 100% of project plans shall include work breakdown structures, critical paths, estimated resources, risk matrices and other elements as required. ▪ 100% of plan schedules and activities shall be coordinated with all required participants. ▪ The contractor shall communicate all issues impacting project schedules to government staff within one business day after determination of impact. ▪ Changes to project plans shall be updated within mutually established time parameters. ▪ 100% of documentation and services (including updates) shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents. ▪ 100% of documentation and services (including updates) shall be completed and submitted IAW the requirements established within the requirement documents.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Project Management Team Facilitation	▪ 100% of facilitation presentations and communications shall be coordinated as required and shall be clear, effective, concise, and organized. ▪ 100% of facilitation activities shall be tailored specifically for team needs and shall result in the team's ability and empowerment to achieve documented action items and milestones. ▪ Facilitators shall respond to 100% of questions and requests with applicable responses/references. ▪ 100% of documentation and services (including updates) shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents. ▪ 100% of documentation and services (including updates) shall be completed and submitted IAW the requirements established within the requirement documents.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Weekly Status Report	▪ 100% complete. ▪ 100% accurate. ▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period.	▪ No more than 1 violation per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Documentation Repository	▪ Current electronic versions of all documentation in the required format shall be posted within the mutually established time parameters in the artifact repository and shall be available for Government review at all times as required.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

CLIN 009 - TASK ORDER MANAGEMENT

1. OVERVIEW

The contractor shall provide complete task order management as required to ensure successful completion of all task order requirements in accordance with the terms and conditions of the task order.

2. SCOPE/DUTIES

The minimum requirements associated with task order management are identified below.

a) The task order management team shall include one Task Order Manager (TOM) whom is responsible for the overall task order performance and whom shall act as the primary liaison between the individual contractor employees and the Government. The name of the primary TOM and alternate(s) TOM, who shall serve as the TOM when the primary TOM is absent, shall be designated in writing to the Contracting Officer (CO) at the time of award.
b) The contractor shall clearly define the duties to be performed by all contractor personnel to ensure a clear distinction between task order management support and operational support that is performed under one or more other Contract Line Item Numbers (CLINs) as described in PWS paragraph 5.1 (i.e. non-task order management). A full explanation with sufficient information demonstrating how the operational duties will not be affected by the task order management duties will be required for all contractor personnel proposed to provide support in multiple areas (i.e support the task order management CLIN and any other CLIN(s)).
c) The Contractor personnel are under the administrative control of the Contractor. The Contractor shall be solely responsible for the complete supervision and management of its personnel under the task order. The Contractor shall select, supervise, and exercise control and direction over its personnel under this task order. The Government shall not supervise, direct, or control the activities of Contractor personnel. The Contractor shall not exercise any supervision or control over the Government in performance of contractual services.
d) The Contractor's TOM shall meet monthly (or more frequently if needed) with the COR or Government project staff to communicate work status; discuss accomplishments or problems; and propose solutions and enhancements of services. The TOM shall identify methodologies and performance schedules to ensure work is progressing satisfactorily. The COR will establish and relay priorities for tasks and projects at these meetings and communicate directly with the TOM. Acceptance criteria, areas of outstanding performance, and any failure to meet task order requirements, along with necessary corrective action, will be discussed and shall be documented.
e) The contractor shall schedule, facilitate, and document a Program Management Review (PMR) each quarter with NITC and GSA representatives for the duration of the task order, unless otherwise directed. The PMR shall be a forum to review and discuss the following: overall task performance including significant accomplishments; issues and

risks; additional areas of needed support; potential resource allocation adjustments; and other items deemed essential at a later date.

f) The contractor shall provide general task order management support to include, but not be limited to, the tasks identified below.
   i. The contractor shall provide a task order management plan that describes the technical approach, organizational resources, and management controls proposed for task performance.
   ii. Manage all overall task performance.
   iii. Assign and manage contractor work schedules to ensure the necessary coverage is provided in accordance with the task requirements.
   iv. Review work discrepancies.
   v. Disseminate communicating policies, purposes and goals of the client organization(s) to contractor personnel providing task order support as applicable.
   vi. Track expiration of system access (LincPass) badges to ensure re-enrollment is accomplished a minimum of 30 days prior to expiration.
   vii. Management, to include scheduling and monitoring, of overall contractor personnel training to ensure compliance with the training requirements identified in PWS paragraph 6.3. Provide the COR and/or the applicable Government representative with a minimum of 30 days advance notice of when employees will be absent for training purposes.
   viii. Complete travel requests (shall use required template) in accordance with the travel requirements identified within PWS paragraph 9.4.2 and ensure sufficient travel funds are available to support such requests.
   ix. Attend meetings beyond those identified in paragraph (d) above.
   x. Notify the ACORT (by telephone or email) when an employee will be absent, within 1 hour of awareness of an unscheduled absence, to minimize any negative impact to daily task activities.
   xi. Maintain up-to-date lists of Government Furnished Equipment (GFE) and Government Furnished Items (GFI). Such lists shall be made available to the Government upon request.
   xii. Development and submission of a monthly status report.
   xiii. Meet with the respective ACORT's on a regular basis, estimated to be bi-monthly, to discuss workloads, progress on projects, and performance issues/problems.
   xiv. Provide a monthly calendar of contractor personnel scheduled absences for the next two months as an appendix to the monthly status report.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Expertise in human resource management, supervision, leadership, conflict resolution, interpersonal skills, and internal controls.
b) Management experience, including expertise in the management and control of funds and resources using complex reporting mechanisms and demonstrated ability in managing multi-task awards and/or subcontract awards of various types and complexity.
c) Experience and expertise in the Information Technology (IT) industry.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Monthly Status Report	▪ 100% complete with all required appendices. ▪ 100% accurate. ▪ Submitted no later than (NLT) 15th calendar day of month following the reporting period and submitted concurrent with the monthly invoice.	▪ No more than 5 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2.500.00	Checklist and Customer Input
Monthly Invoice	▪ 100% complete with all required supplemental information. ▪ 100% accurate. ▪ Submitted no later than (NLT) 15th calendar day of month following the reporting period and submitted concurrent with the monthly status report.	▪ No violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each violation will result in a payment reduction of 5% up to the maximum reduction of $10,000.00.	Checklist and Customer Input
Scheduled Absence Calendar Availability	▪ A current electronic version shall be available for Government review at all times. ▪ The calendar shall be 100% accurate.	▪ No violations per month. ▪ A violation is an error (including grammatical errors), omission, or unavailability.	▪ CPARS assessment ratings. ▪ Each violation will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

LincPass Status	▪ No expirations of valid LincPass accounts.	▪ No violations per month.	▪ CPARS assessment ratings. ▪ Each violation will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Other Task Specific Requirements and Deliverables	▪ 100% adherence to mutually agreed upon management tasks, activities, and objects established and documented in the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.). ▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents. ▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents.	▪ No more than 1 violation per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings.	Checklist and Customer Input

Mandatory Government Training Compliance	▪ 100% of the training (for all contractor personnel performing under the task order, including all CLINs) shall be completed and submitted NLT the established date for training completion as mandated by the Government.	▪ No violations per month.	▪ CPARS assessment ratings. ▪ Each violation will result in a payment reduction of $1,000 up to the maximum reduction of $15,000.00.	Checklist and Customer Input
Security Requirements	▪ Background investigations for 100% of contractor personnel proposed to support task performance shall by favorable.	▪ No violation per month.	▪ CPARS assessment ratings. ▪ Each violation will result in a payment reduction of $3,600.00 up to the maximum reduction of $7,200.00.	Checklist and Customer Input
Personnel Availability	▪ 100% contractor personnel availability during required daily core hours or specific CLIN required schedules (with the exception of coordinated absences). ▪ The contractor is responsible for resource substitution/coverage when a coordinated absence is greater than five consecutive work days.	▪ No more violation per month.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	

Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

Personnel Retention	▪ 100% compliance with staffing requirements identified in PWS paragraph 6.4.	▪ No violations per month. ▪ No more than 10% personnel turnover (on an individual basis, not positional basis) within an annual performance period.	▪ CPARS assessment ratings.	Checklist and Customer Input

CLIN 011 - TECHNICAL ARCHITECTURE SUPPORT SERVICES

1. OVERVIEW

The objective of this is to obtain technical architectural support services to design and create hardware and software architectural and infrastructural designs and technology roadmaps for the USDA's Office of the Chief Information Officer (OCIO), National Information Technology Center's (NITC) Enterprise Data Center (EDC), Enterprise Architecture Branch. The architectural support services shall include the investigation of new technologies and the design of large-scale and complex information technology architectures and infrastructures for which there may be no precedent, including implementation, benchmarking and testing of these new technologies. The contractor support personnel shall also act as a technical liaison between the operations divisions and business divisions with regards to the accompanying business processes that enable the USDA, and other federal Agencies and Departments, to achieve their goals and objectives of eGovernment, leveraging investments and delivering government services in a more citizen-centric manner.

The services offered by the NITC EDC are enterprise-wide. Department, Agency, or Federal eGovernment initiatives can leverage these services. Federal departments and Agencies and their initiatives do not have to create their own technology solutions and standards and can instead utilize the NITC EDC centralized service offerings to support their business requirements and thus avoid the high cost and high learning curve of operating these solutions independently.

The contractor may be required to make contacts with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

a) Creation of detailed network design documents and technology roadmaps.
b) Creation of highly detailed documents which detail business requirements and how they relate to technical designs, specifications and solutions; to include development of technology roadmaps, technological standards, white papers, and complex architectural and infrastructural design documents.
c) Installation, configuration and management of software on Unix, Linux or Microsoft Windows Server operating system.
d) Design, installation, configuration and maintenance of a virtual desktop infrastructure service.
e) Design, installation and configuration of relational database management systems.
f) Creation and maintenance of data center capacity management plans for Infrastructure as a Service, Platform as a Service, and storage platforms.
g) Design, implementation and maintenance of security policies and settings on applications, services or systems being designed.
h) Design, implementation and configuration of enterprise scale storage platforms (e.g. SAN, NAS, CEPH).

i) Design, implementation, configuration and maintenance of virtualization platforms (e.g. VMWare ESX, KVM, Xen).
j) Design, implementation and configuration of IT security systems, services and sub-systems (I.e. firewalls, IDS/IPS, UTM, log aggregation).
k) Design of web services, associated data dictionaries, connectors and adapters (e.g. SOA, SAML, REST, SOAP, HTTP, HTTPS, UDDI, SSL, TLS, XML, WSDL, ESB).
l) Troubleshoot complex issues within networks, server operating systems, storage subsystems or security subsystems.
m) Design and implementation of cloud-based services such as email, messaging, server virtualization, storage virtualization and network virtualization.
n) Integration of disparate systems and subsystems with little or no known precedent.
o) Implementation of, or adherence to, enterprise architecture processes.
p) Implementation, configuration and maintenance of LDAP and LDAP design and integration.
q) Design and implementation of architecture and infrastructure lifecycle management plans.
r) Creation of white papers, executive summaries, and written technical presentations for senior and executive IT management.
s) Use of collaboration tools to capture documentation and design artifacts (i.e. Wiki, Git).
t) Creation of Virtual Desktop Infrastructure (VDI) designs and its implementation and documentation.
u) Create documentation, white papers, and presentations related to assigned research of new and emerging technologies.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Experience with Network Design.
b) Experience with Unix, Linux, and Microsoft Windows server operating systems.
c) Experience with administering, or integrating with, relational database management systems.
d) Experience creating data center capacity management plans.
e) Knowledge of IT security principles and practices.
f) In-depth knowledge of enterprise scale storage platforms (e.g. SAN, NAS).
g) Management and/or design of virtualization platforms (e.g. VMWare ESX, KVM, Xen).
h) In-depth knowledge of web services (e.g. SOA, SAML, REST, SOAP, HTTP, HTTPS, UDDI, SSL, TLS, XML, WSDL, ESB).
i) Extensive troubleshooting and logical skills.
j) Experience with Cloud architectures and technologies.
k) Knowledge of systems integration principles and practices as well as interoperability concepts.
l) Experience with enterprise architecture processes.
m) Knowledge of LDAP and LDAP design and integration.
n) Knowledge of Citrix and/or VMWare View software and technology
o) Knowledge of architecture and infrastructure lifecycle management plans.
p) Excellent written and oral presentation skills.

4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Technology Analysis Deliverables and Tasks	▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.), to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.	▪ No more than 6 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Design and Implementation Planning Deliverables and Tasks	▪ 100% of documentation shall be clear, concise, organized and developed with required tools as applicable. ▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.	▪ No more than 6 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Documentation Updates and Storage/Repository	▪ 100% of documentation shall be updated IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance. ▪ Electronic versions of all documentation in the required format shall be posted/stored within mutually established time parameters in the required artifact repository/tool location and shall be available for Government review at all times as required.	▪ No more than 6 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Performance Benchmark Test Deliverables And Tasks	▪ 100% of documentation shall be clear, concise, organized and developed with required tools as applicable. ▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.	▪ No more than 6 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Collaboration Deliverables and Tasks	▪ 100% attendance and active participation in all collaboration events as required. ▪ 100% of collaboration communications shall be clear, effective, concise, and organized. ▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.	▪ No more than 6 violations per month. ▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Weekly Status Report	▪ 100% complete. ▪ 100% accurate. ▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period.	▪ No more than 1 violation per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $2,500.00.	Checklist and Customer Input
Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 6 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.	Checklist and Customer Input

Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

CLIN 012 - TECHNICAL WRITER

1. OVERVIEW

The objective is to obtain Information Technology (IT) technical documentation support to help the National Information Technology Center (NITC) develop, maintain and update critical documents at the NITC Enterprise Data Center. This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

The contractor shall create and/or maintain a variety of documentation, including, but not limited to, workflow (swim lane) documents, functionally specific technical templates, technical solution proposals, standards documents, presentation materials, and metric reports, etc. The contractor shall update and/or reformat existing documentation and develop new formats to comply with new regulations, directives, or guidance. Upon completion, all documentation shall be finalized and accurate, and remain current through periodic reviews and updates.

The documentation to be prepared includes, but is not limited to, the following:

- System documentation
- Certification and Accreditation
- Security documentation (including security plans, risk assessments, trusted facility manuals, security features users guide, and privacy impact assessments)
- Operating instructions/processes and user guides
- Standard operating procedures
- Disaster Recovery plans
- Internal controls
- Hardening Guidelines/Guides
- Operation Level Agreements /Service Level Agreements (OLAs/SLAs)
- Service Catalog descriptions and appendices

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Recent (within previous 12 months) experience with IT technical writing and creating IT technical documentation.
b) Expert knowledge of various tools such as Microsoft Office suite (Word, Excel, and PowerPoint), SharePoint, Wiki, etc.
c) Proven ability to manage multiple assignments and ability to adapt to stringent or flexible deadlines.
d) Effective communication (written and oral) and organizational skills.

4. **PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE**

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Task Specific Requirements and Deliverables	▪ 100% adherence to mutually agreed upon tasks and activities established and documented in the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.). ▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each violation will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input
Inquiry Response	▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.	▪ No more than 2 violations per month. ▪ A violation is an error (including grammatical errors), omission, or delayed delivery.	▪ CPARS assessment ratings. ▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.	Checklist and Customer Input

Security Incident Notification and Resolution	▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.	▪ No allowable violations per month.	▪ CPARS assessment ratings. ▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.	Checklist and Customer Input

CLIN 013 - ADDM ADMINISTRATION & MODELING SERVICES

1. OVERVIEW

The objective is to obtain Information Technology (IT) technical support for the National Information Technology Center (NITC) IT Service Management Branch, Infrastructure Operations Division (IOD/ITSMB). The contractor shall provide BMC Software Atrium Discovery and Dependency Mapping (ADDM) system administration and application modeling services for the support and management of the ADDM software product and supporting infrastructure. ADDM, an IT Asset discovery tool, discovers physical and virtual IT assets, applications, and the relationships between them. The contractor may be required to make contacts with NITC customers, technical staff, business partners, management, and internal/external auditors.

2. SCOPE/DUTIES

System Administrative Services

a) Install, configure, manage and maintain the BMC ADDM product.
b) Setup and install ADDM virtual appliance.
c) Setup and install Windows discovery slaves.
d) Run discovery in Open Systems and Windows environments and interpret results.
e) Consolidate discovered data from multiple appliances to a single appliance.
f) Setup users and work with security to configure User Interface (GU) security.
g) Configure and customize reports in dashboards and report channels.
h) Access and configure dashboards.
i) Diagnose and troubleshoot discovery issues.
j) Backup discovered data using snapshots, as required.
k) Configure and customize integration to BMC Atrium CMDB.
l) Configure a static integration point to import business contextual data.

Application Modeling Service

a) Manipulate the Tideway Query Language, Data Model and Operating Principles.
b) Development and testing of Tideway Pattern Language (TPL) patterns for application modeling in test environments.
c) Analyze, document and manage customer requirements for new ADDM application modeling requests including necessary TPL pattern changes or additional configuration item mapping.
d) Manage all software components - uploading all code, scripts and documentation to ADDM portal (version control system).
e) Test patterns with manual pattern execution.
f) Write advanced search queries to report data required.
g) Extract data using XPath and regular expressions.
h) Design and implement successful triggers.

i) Manage detailed Technology Knowledge Update (TKU) (TKU testing every month - analysis of new/amended patterns and TPL code).
j) Manipulate the TPL patterns and use these along with provenance data to calculate reasons as to why software product data is either missing or appears to be incorrect.
k) Respond to client requests for troubleshooting software data quality issues in ADDM (i.e. incorrectly discovering Oracle TCP ports, missing version information on software, etc.).
l) Enhance and test core ADDM discovery scripts and ensure that scripts are modified to ensure that elevated privilege commands and path variables are correct as per the environment.
m) Research the latest ADDM product versions and upcoming technology, including but not limited to, taxonomy extensions for additional data store nodes, attributes relationships and UI modifications.
n) Document ADDM modeling, daily operational activities and procedures, and other items as required.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Hands on experience in mid-range operating system administration on the mid-range platform servers including Solaris, Linux, AIX and Windows.
b) Knowledge of TCP/IP, IP Subneting, DNS, network architecture/routing and security/firewall policies.
c) Expert level experience with BMC ADDM 9.0 or higher System Administration & Application Modeling.
d) Hands on experience with other IT discovery industry marketed asset discovery products.
e) Certified in ITIL Foundations v3.
f) Knowledge of Visual Basic for Applications (Access 2003).
g) Database management and database design.
h) Interpersonal skills both verbal and written.
i) Ability to manage multiple projects.
j) Proficiency in MS Office products.

CLIN 014 - APPLICATION INTEGRATION ENGINEERING SUPPORT SERVICES

1. OVERVIEW

The objective is to obtain technical support for critical customer hosted applications in the National Information Technology Center (NITC) Platform as a Service (PaaS) environment. This includes supporting Commercial Off The Shelf (COTS) product environments as well as customer custom integrations in those COTS environments. The contractor shall support the System Integration Branch (ASID/SIB). The contractor may be required to make contact with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

a) Request Linux/Unix/Windows servers per NITC processes.
b) Install Commercial-off-the-Shelf (COTS) software per vendor recommendations.
c) Configure COTS software per vendor, NITC, or customer requirements.
d) Review patch levels of COTS software at least quarterly and install versions per vendor recommendations.
e) Monitor Incident and Service Request queue and perform work per customer/NITC requirements in the timeframe requested.
f) Adhere to NITC Incident and Change Management processes for all activities performed on behalf of customers.
g) Design solutions based on customer requirements.
h) Create high-level task lists to implement customer designs.
i) Communicate and report on tasks associated with customer implementation projects. Examples of COTS packages currently supported:
   - Web Application Servers: WebSphere, WebLogic, Tomcat, JBoss, Apache
   - Content Management: Oracle WebCenter Content, Drupal, Alfresco
   - Portal: WebSphere Portal
   - Business Intelligence: Oracle EPM, Oracle OBIEE, IBM Cognos
   - Search Tools: Google Search Appliance
   - Social Media Tools: IBM Lotus Connections
   - Other: IBM Tivoli Usage and Account Manager, BMC Remedy, HP LoadRunner

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) In-depth, recent (within the past year) hands-on experience with similar commercial COTS software listed above.
b) Experience working independently and as part of a project team with deploying, maintaining, and supporting customer custom applications in a COTS environment.

4. ADDITIONAL INFORMATION

The Government estimates that varying levels and types of requisite skill sets will be required to complete the stated requirements. The Government is providing historical

information to illustrate the types of skill sets and the level-of-effort in terms of Full-Time-Equivalent (FTE) positions that have been utilized to support past requirements.

Product Area	Number of FTE	General/Estimated Skill Level
WebSphere	5	3 senior / 2 junior
Oracle UCM/WebCenter Content	2	1 senior / 1 junior
WebSphere Portal	2	2 senior
Oracle Hyperion/EPM	2	2 senior
Google Search Appliance	1	1 senior
IBM Lotus Connections	1	1 senior
IBM Tivoli Usage and Account Manager	1	1 senior
BMC Remedy	1	1 senior
Endpoint Encryption	0	0 senior

CLIN 015 - DATA CENTER HARDWARE SUPPORT SERVICES

1. OVERVIEW

The objective is to obtain Information Technology (IT) technical support for the National Information Technology Center (NITC) Enterprise Data Center (EDC) floor activities and processes, including infrastructure and hardware, as required. The contractor may be required to make contact with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

The contractor shall support and complete tasks as required for all aspects of the following activities: hardware installation; de-installation; removal; relocation; power; rack and stack; receiving and disposal; project milestone development and management, task identification and documentation; as-built diagrams; EDC processes; change/problem management; implementation techniques; and hot site disaster recovery exercise documentation and demonstration. Task specific requirements include, but are not limited to, those identified below.

a) Determine, identify and coordinate electrical power requirements for new and existing IT hardware in the NITC Enterprise Data Center.
b) Coordinate IT hardware placement, installation, move, replacement, and removal activities.
c) Create and maintain documentation for NITC Enterprise Data Center IT hardware and infrastructure systems using tools that include but are not limited to the following: Microsoft Office products, Remedy ITSM Suite with integrated products and AutoCAD.
d) Support NITC system maintenance windows.
e) Submit recommendations and justifications to modernize or improve data center infrastructure systems and IT hardware management. Provide recommendations, analysis and reviews of performance profile surveys, equipment inspections, technical troubleshooting, maintenance evaluations, and workload analysis.
f) Troubleshoot, research, and analyze IT hardware, system integration and/or system component issues.
g) Evaluate and determine the quality and quantity of IT hardware repair parts and tools to reduce unnecessary duplication and variety, as well as to ensure that needed materials are on hand.
h) Responsible for IT hardware ingress and egress from the NITC Data Center facility:
    i. Receive, unload and store NITC internal, customer and vendor IT hardware delivered shipments at the time of NITC facility arrival according to documented Change and Service Asset and Configuration Management processes and procedures.
    ii. Plan, pack and coordinate the removal of disposed or excessive IT hardware in accordance with established procedures, including notification to Resource Management as required.

i) Perform IT hardware installation according to documented Change and Service Asset and Configuration Management processes and procedures.
j) Participate in weekly NITC Enterprise Data Center (EDC) Board reviews.
k) Conduct physical inventory of IT equipment for NITC EDCs, as required.
l) Report, coordinate and resolve hardware configuration item data discrepancies or updates within the Service Asset and Configuration Management processes.
m) Escort internal IT staff and external customers with limited or no security clearances into NITC EDC secured data center facility and assist with or monitor routine or emergency IT hardware maintenance activities.
n) Daily monitoring of the NITC enterprise data center environmental conditions (CRAC units), cooling systems and data center power controls to include the reporting of issues to NITC Facilities Manager and other NITC personnel as required.
o) Monitor and ensure adherence to appearance and safety standards within the NITC data center facility, in accordance with NITC Data Center and access policy and procedures. All non-compliance issues shall be reported to the federal EDC Floor Manager.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Overall project management of secure data center projects with the ability to manage multiple projects simultaneously.
b) Moderate IT service and hardware field maintenance.
c) Proven analytical, problem-solving and hardware troubleshooting skills.
d) Able to physically and safely lift 50 LB.

CLIN 016 - DATABASE ADMINISTRATION (DBA) SERVICES

1. OVERVIEW

The objective is to obtain technical services required for the administration, installation, maintenance, securing, and deletion of database products, including but not limited to COTS products, in support of the Information Services Division (ISD), Database Management Branch (DMB). The contractor may be required to contact National Information Technology Center (NITC) customers, technical staff, business partners, management, and internal and external auditors. The contractor shall provide local and remote systems DBA support for various mainframe and mid-range databases and database related products.

2. SCOPE/DUTIES

The contractor shall provide systems database administration support in a variety of areas including but not limited to the following: monitoring, analyzing, troubleshooting, diagnosing, securing, encrypting, tuning and maintaining DB2, MySQL, Oracle, Adabas, and/or SQL Server and related database products including integration with tools or other software within the database product suite.

NITC currently supports DB2 on Windows, AIX, Linux, VMWare and mainframe platforms; MySQL on Windows and Linux; Oracle on Windows, AIX, Solaris, and Linux; Adabas on mainframe; and SQL Server on Windows and VMWare. Clustering on multiple servers shall be supported.

NITC generally provides full system database administration support for its managed hosting and platform-as-a-service customers. NITC's customers generally perform application administration; however, NITC often provides support in this area as requested by customers.

NITC technicians also provide customers with assistance and/or guidance on hardware configuration and support. The contractor shall support after hours and weekend support to perform hardware and software maintenance as required.

The task requirements to be supported and completed by the contractor include, but are not limited, the following:

a) **Non-Mainframe Environments**. The contractor shall provide comprehensive Database support in the non-mainframe environment, which shall include but is not limited to the tasks/products/tools as identified below. Specific tasks are further identified in subsequent paragraphs.

- Installation of the database software.
- Creation of installation scripts for the database software.
- Installation of and corrective action for the database software and tools as well as creation of the instance and/or database.

- Provide analysis data to the agency/customer such that the customer can adequately determine when to use a partitioned/clustered database.
- Provide analysis data to the agency/customer such that they can adequately determine when to use special types of data containers and the placement of those containers.
- Monitoring, analysis and tuning of the instance and/or database for maximum performance.
- Granting and/or revoking of privileges required to create and maintain the tables, indexes and other structures needed to store the customer's data to a select group of personnel designated by the customer.
- Recover the instance and/or database in case of a disaster scenario or a disaster test scenario.
- Execution of normal duties described commonly for an application DBA, such as creation of tables, indexes, etc.
- Binding of application software packages.
- Monitoring, analysis and tuning recommendations for the application layer, even when not making a change to a database.

i. ***MySQL Administration***. Specific tasks and support areas include, but are not limited to, the following:

- Ensure connectivity and availability.
- Install database software.
- Configure database software.
- Create/configure backup and restore scripts.
- Removal of database and software in accordance with policies established by the Government.
- Database restoration using full, differential, and log backups.
- Data extraction/transformation/load (ETL).
- Working with external and remote data.
- Clustering.
- Working with metadata.
- Retrieving XML result sets.
- Analyzing query plans.
- Client connectivity.
- Configuring client/server network libraries.
- Using extended Stored Procedures.
- Managing indexes and locks.
- Troubleshooting deadlocks.
- Working with statistics.
- Scripting.
- Creating alerts.
- Database design.
- Database install/upgrade/configuration.
- Schema management.
- Performance monitoring.
- Backup/recovery planning.

- SQL tuning.
- Data replication.
- Database reorganization.
- Data loading.
- Database coding/maintenance, optimization.

ii. ***Oracle Administration***. Specific tasks and support areas include, but are not limited to, the following**.**

- Detailed design plans.
- Utilization of system design plans.
- Planning and specifications.
- Install database(s) and associated applications using all tools.
- Preparation scripts for RAC deployments.
- Pre-Install testing and problem resolution for RAC deployments.
- Configuration.
  - Configure and maintain database structures.
  - Configuration control and capacity planning activities.
- Customize Oracle databases.
- Optimize Oracle databases and applications.
- Patch Oracle databases.
- Secure and harden Oracle databases.
- Test & verify.
  - Maintain database(s) and associated applications using all tools.
- Routine/preventative maintenance activities.
  - Backups – establish and monitor.
  - Recovery Procedures – establish and monitor.
- Monitoring security of the databases down to application layer.
- Database and application and security related patches/fixes.
- Departmental standards and regulations regarding patching/fixpacks.
- Upgrades of Oracle databases.
- License compliance – ensuring application revision level is at current industry level as allowed by current maintenance agreement with vendor (Oracle).
- Maintaining database dictionaries and integration of system through database design.
- Monitoring availability, performance and compliance with software licensing.
- Queries – development, maintenance and tuning.
- Performance tuning of system/application.
- Reports – development and maintenance.
- Capacity management.
- Coordination of changes.
- Analysis, review and maintenance of secure logins to and associated applications.
- Connectivity from clients.
- Optimization of performance to exceed NITC requirements for user accessibility.

- Logs – monitor and maintain critical database logs and standard parameters in order to maintain reliable and consistent database operations.
- Problem Management.
  - Troubleshoot/Debug/update problem ticket(s).
  - Correct/Replace HW.
- Oracle Database.
  - Assist development team for new release deployments.
  - Install, configure and test Oracle Disaster recovery environment.
- Oracle RAC.
  - Install, configure and maintain Oracle cluster environment.
  - Configure and maintain SAN devices using Oracle Automatic Storage Manager (ASM).
- Oracle Grid.
  - Install and configure Oracle Grid control server.
  - Install and integrate agents on all the Oracle systems.
  - Enable automatic performance.
- Oracle Middleware.
  - Install, configure and maintain web logic server (needed for grid control toolset).
  - Oracle App Server, Oracle Forms & Reports.
  - Oracle Internet Directory/LDAP/Single Sign-on.
- Oracle Tools.
  - Install, configure and maintain Oracle Data Integrator, Oracle Warehouse Builder, Oracle business intelligence tools.

iii. ***DB2LUW Administration***. Specific tasks and support areas include, but are not limited to, the following**.**

- Working with metadata.
- Retrieving XML result sets.
- Analyzing query plans.
- Client connectivity.
- Configuring client/server network libraries.
- Using extended Stored Procedures.
- Managing indexes and locks.
- Troubleshooting deadlocks.
- Statistics.
- Scripting, creating alerts.
- Partitioned views.
- Optimization.
- Database design.
- Database install/upgrade/configuration.
- Schema management.
- Performance monitoring.
- Backup/recovery planning.
- SQL tuning.

- Data replication.
- Database reorganization.
- Data loading.
- Database coding/maintenance.

iv. ***SQL Server Administration*.** Specific tasks and support areas include, but are not limited to, the following**.**

- Installation, administration, tuning and removal of SQL Server Enterprise Edition latest release or one release back; SQL Server Enterprise Manager and SQL Query Analyzer.
- Scheduling jobs with SQL Server Agent.
- SQL Server Storage Structures.
- Index and Security Architecture.
- SQL Profiler.
- Database restoration using full, differential, and log backups.
- Data extraction/transformation/load (ETL).
- Working with external and remote data.
- Clustering.
- Working with metadata.
- Retrieving XML result sets.
- Analyzing query plans.
- Client connectivity.
- Configuring client/server network libraries.
- Using extended Stored Procedures.
- Managing indexes and locks.
- Troubleshooting deadlocks.
- Working with statistics.
- Scripting.
- Creating alerts.
- Database design.
- Database install/upgrade/configuration.
- Schema management.
- Performance monitoring.
- Backup/recovery planning.
- SQL tuning.
- Data replication.
- Partitioned views.
- Database reorganization.
- Data loading.
- Database coding/maintenance, optimization.

b) **Mainframe Environment**. The contractor shall provide comprehensive Database support in the mainframe environment, which shall include but is not limited to the products/tools as follows:

- DB2
- DDF
- DRDB – Distributed Replicated Block Device (for Linux)
- ICSF – Integrated Cryptoprocessor Service Facility
- DB2 Grouper
- DB2 DAE – Database Archive Export
- Query Patroller
- RRS – Resource Recovery Service (comes with mainframe), used by NITC with stored procedures
- TPCH db – benchmark tool
- HADR – High Availability Disaster Recovery
- Utilities & Tools for LUW – commands/utilities used by NITC
- PD/PSI – Problem Determination/Problem Source Identification
- DART – Database Analysis Reporting Tool
- TSA – Tivoli System Automation
- IBM QMF current release
- BMC ALTER current release
- IBM DB2 PM current release
- IBM Optim (formerly Archive) for DB2 current release
- Health monitor
- System monitor
- Snapshot
- DRDA – Distributed Relational Database Architecture
- IBM DB2 Connect
- IBM DB2 High Performance Unload (HPU)
- Other database or related products to be supported include, but are not limited to, the following:
  - ADABAS
  - ComPlete
  - Natural
  - Review
  - Predict
  - Native SQL
  - EntireX
  - Finalist
  - Focus
  - IDMS
  - DPV
  - Other Software AG middleware products

c) **Ancillary Software**. Ancillary software is defined as non-database software sold by database vendors. Tasks include, but are not limited to, the following:

- Perform administrative functions such as create/delete user accounts, set passwords, troubleshoot problems, etc.

- Provide developer support to customers who use customized databases; this includes understanding the needs of the customers who use customized databases to enable the development, modification and testing of the databases and change tracking.
- Provide guidance on the configuration of the ancillary products to ensure incorporation of "best practices" in designs.
- Provide documentation and knowledge transfer to the Government.
- Perform routine/preventative maintenance activities.
  - Backups – establish, monitor and document.
  - Recovery Procedures – establish, monitor and document.
  - Harden and monitor security of the middleware application; ensure the middleware application and security related patches/fixes are up to date as determined by departmental standards and regulations.
- Patching completed in accordance with the guidelines established by the Government.
- Upgrades - ensure application revision level is at current industry level as allowed by government licensing.
- Maintain middleware dictionaries and integration of system through application design.
- Monitor performance and compliance of middleware.
- Performance analysis and tuning of System/Application (middleware).
- Reports – develop and maintain.
- Capacity management.
- Security.
  - Coordinate changes to the proper OS team to effectively administer middleware applications with server security requirements as determined by departmental standards.
  - Analyze, review and maintain secure logins to middleware applications and their associated applications.
- Change Management process compliance.
- Logs - monitor and maintain critical middleware logs.
- Problem Management.
  - Troubleshoot/Debug.
  - Correct/Replace HW.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Recent experience (within the past 12 months) with applicable database products (DB2, Oracle, SQL Server, MySQL, etc.). Certifications are preferred, but not required.
b) MySQL Server Administration. Contractor personnel supporting task requirements shall have demonstrated experience with the specific products and activities identified in paragraph (2)(a)(i) above. Experience as an application developer/programmer or application DBA is desired but not required.
c) Oracle Administration. Contractor personnel supporting task requirements shall have demonstrated experience with the specific products and activities identified in paragraph (2)(a)(ii) above. Experience as an application developer/programmer or application DBA is desired but not required.

d) DB2LUW Administration. Contractor personnel supporting task requirements shall have demonstrated experience with the specific products and activities identified in paragraph (2)(a)(iii) above. In addition, the following requirements apply:
   - DB2 expertise and experience with the utilization of monitoring, diagnostics, and analysis tools.
   - Korn Shell, Perl, Java, J2EE, and C programming/scripts experience.
   - Knowledge of IBM Tivoli Storage Manager and Symantec Veritas Netbackup.
   - Experience executing native DB2 commands and utilizing GUI.
   - Experience as an application developer/programmer or application DBA is preferred but not required.

e) SQL Server Administration. Contractor personnel supporting task requirements shall have demonstrated experience with the specific products and activities identified in paragraph (2)(a)(iv) above. Experience as an application developer/programmer or application DBA is desired but not required.

f) Mainframe. Contractor personnel supporting task requirements shall have demonstrated experience with the specific products and activities identified in paragraph (2)(b) above. Experience as an application developer/programmer or application DBA is desired but not required

4. ADDITIONAL INFORMATION

The Government estimates that varying levels and types of requisite skill sets will be required to complete the stated requirements. The Government is providing historical information to illustrate the types of skill sets and the level-of-effort in terms of Full-Time-Equivalent (FTE) positions that have been utilized to support past requirements.

Product Area	Number of FTE	General/Estimated Skill Level
SQL Server	3	1 Senior / 2 Intermediate
Oracle	3	2 Senior / 1 Intermediate
Mainframe	1	1 Senior
DB2LUW/MySQL	1	1 Senior

CLIN 017 - MAINFRAME SYSTEMS PROGRAMMING SERVICES

1. OVERVIEW

The objective is to obtain technical support services for z/OS and Commercial Off the Shelf (COTS) software installation and problem analysis of various mainframe based products for the National Information Technology Center (NITC), Systems Engineering Division, Mainframe Systems Branch (SED/MSB). The contractor may be required to make contact with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

The contractor shall support all aspects of product installation, including but not limited to, project milestone development and management, task and software documentation, data set naming convention, installation process, data copy and migration techniques, coding, dynamic activation and interrelationships with other PARMLIB or APF library members, product administration, change/problem management, implementation techniques, and hot site disaster recovery exercise documentation and demonstration. Task specific requirements include, but are not limited to, those identified below.

a) Utilize IBM's SMP/E software products installation and maintenance utility process.
b) Utilize IBM's Job Control Language (JCL) and utility programs (i.e. IEBGENER) to maintain z/OS software products.
c) Utilize IBM's file structure(s): (i.e. HFS, ZFS, and PDS's).
d) Utilize TSO ISPF panels.
e) Utilize IBM's SDSF and/or equivalent ISV product.
f) Utilize IBM data storage product DFSMS.
g) Technical consulting and analysis of new technologies, implementation strategy, and impact to production.
h) Independently diagnose and resolve trouble calls in technical areas.
i) Develop technical specifications, in accordance with established requirements and schedules.
j) Develop and implement technical documentation, in accordance with established requirements and schedules.
k) Review proposed policy, regulations, and procedural changes to determine impact on area of responsibility.
l) Develop on the job training (OJT) programs on new developments in technology and software packages.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Sufficient experience necessary to accomplish z/OS mainframe systems programming activities (including integration) and client consultation.
b) Extensive hands-on experience as a z/OS mainframe system programmer.

CLIN 017 - NETWORK ENGINEERING SERVICES

1. OVERVIEW

The objective is to obtain technical, on-site support for the National Information Technology Center (NITC) for the General Support System (GSS) Network components, within the Information Services Division, Network Services Branch (ISD/NSB). This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

The Contractor shall support the operations and configuration management of the telecommunications infrastructure, including but not limited to, computer system/network design and engineering requirements. Specific tasks include, but are not limited to, the following:

a) Enterprise Network Infrastructure Implementation: Coordinate work with NITC platform teams and network teams to improve enterprise tool sets for performance monitoring, alert monitoring, event correlation and suppression, ticket notification and escalation. Test and analyze elements of the network infrastructure, including NITC's network management solutions that support the enterprise network.
b) Enterprise Network Infrastructure Reporting: Monitor and control the performance and status of the network resources (performance is affected by modifying the configuration files to streamline the network data flow). Utilize software and hardware tools and identify and diagnose complex problems and factors affecting network performance. Generate network enterprise reports to management on the overall performance of the GSS Network.
c) State of the Art Enterprise Solutions: Research industry offerings and remain up-to-date with telecommunication infrastructure offerings to provide expert advice regarding future enterprise networking solutions.
d) Change/Incident Management: Comply with NITC's stated policies and procedures for Change/Incident and Asset Management. Utilize the NITC's standardized tools to document problems and request changes to any part of the network infrastructure.
e) Disaster Recovery: Participate as a network technical lead to support NITC's Disaster Recovery, to include exercises, at remote site, in Kansas City or on-site support at the disaster recovery facility (in St. Louis, MO and Beltsville, MD) as outlined in NITC's disaster recovery plan.
f) Assessment and Authorization (A&A): The contractor shall provide technical input for the A&A of the NITC's enterprise network. The contractor shall write technical documents that include network diagrams, to support NITC's ongoing A&A accreditation as required. The contractor shall provide information identifying the actions necessary to rectify security exploitations in response to audit findings. Additionally, the contractor shall document and complete corrective actions related to such findings as required.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Computer system/network design, engineering, and support, including specialized experience related to networking tasks.
b) Physical Layer Infrastructure deployment/troubleshooting (cabling infrastructure).
c) Data Link Layer (network switching).
d) Network Layer routing protocols (network routers and associated protocols).
e) Transport Layer protocols (TCP/UDP).
f) Load Balancer configuration tasks.
g) IP Addressing (IPV4 and IPV6).
h) Running and deciphering packet captures.
i) Familiarization with network Firewalls and their operation.
j) Configuring and managing/troubleshooting Access Control Lists.
k) Network Management tasks.
l) DNS Management.
m) Network monitoring.
n) Network virtualization tasks.
o) Software-defined network configuration tasks.
p) Documenting network environment and automated processes.
q) Implementing security controls.
r) Developing project plans/tasks lists.

CLIN 019 - REMEDY ENGINEERING AND ADMINISTRATON SERVICES

1. OVERVIEW

The objective is to obtain Information Technology (IT) technical support for the National Information Technology Center (NITC) IT Service Transition team. The contractor shall manage the various Remedy engineering and administration duties within the Infrastructure Operations Division, IT Service Management Branch. The position is responsible for on-going maintenance, configuration, development and customizations of the NITC enterprise, multi-tenant Remedy IT Service Management (ITSM) Suite with integrated software products utilizing NITC software development lifecycle methodology. This position may require making contacts with NITC customers, technical staff, business partners, management, and internal/external auditors.

2. SCOPE/DUTIES

a) Perform the installation, upgrade, configuration, application development, and/or customization, administration and integration of the BMC ITSM Remedy based applications (v7.6 or higher) including AR System (v7.5 or higher), Incident Management, Change Management, Problem Management, Service Request Management (SRM), Service Level Management (SLM) and Asset Management and Atrium Configuration Management Database (CMDB).
b) Perform Remedy IT Service Management Suite v7.6 or higher including AR System v7.5 application support including developing technical documentation, assisting with the development of end-user documentation, interfacing with application owners and the Service Desk, and properly tracking all support efforts
c) Provide development and support of one or more product integrations to BMC ITSM Remedy Suite such as but not limited to, BMC Atrium Discovery Dependency Mapping v8.0 or higher (ADDM), BMC ProactiveNet Performance Management (BPPM), BMC BladeLogic Server Automation 8.0 and Atrium Orchestrator.
d) Collaborate and/or coordinate with functional and technical groups to translate business requirements into technical design documents.
e) Assist in the definition of business, functional and technical requirements, determine scope, estimate work effort and determine duration of development activities.
f) Participate in design and peer reviews boards.
g) Transfer knowledge to the Government and customers as requested.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Administrative level experience consisting of installing, configuring and administrating the BMC ITSM Remedy based applications (v7.6 or higher) with AR System (v7.5 or higher) including Incident Management, Change Management, Problem Management, Service Request Management (SRM), Service Level Management (SLM) and Asset Management and Atrium CMDB.
b) Application development experience enhancing out-of-the-box BMC ITSM Remedy based applications (v7.6 or higher) including AR System (v7.5 or higher), Incident Management, Change Management, Problem Management, Service Request

Management (SRM), Service Level Management (SLM) and Asset Management and Atrium CMDB.

c) Application customization experience customizing new forms, objects, workflow, etc. layered with out-of-the-box BMC ITSM Remedy based applications (v7.6 or higher) and AR System (v7.5 or higher) including Incident Management, Change Management, Problem Management, Service Request Management (SRM), Service Level Management (SLM) and Asset Management and Atrium CMDB.
d) Hands on experience with Tier 2 and Tier 3 support model in IT Operations mission critical 24x7 environment.
e) Expert level troubleshooting, analytical and problem solving skills.
f) Good communications and interpersonal skills, both verbal and written.
g) Mastery of the Microsoft suite to include Office, Excel, Word, PowerPoint and Visio.
h) ITIL Foundation v3 certified.
i) Experience with Remedy mid-tier, AR system and database performance tuning/performance optimization.
j) Systems administration, infrastructure engineering, and network/security engineering, database and data management experience is preferred.
k) Experience with ITSM Analytics (8.0 or higher), Business Objects Enterprise (BOE), Dashboards for BSM 2.5.01 and Crystal Reports preferred.
l) Experience with SQL queries/reports from MS SQL Databases.

CLIN 020 - SECURITY ADMINISTRATION SERVICES - ACTIVE DIRECTORY (AD) AND IDENTITY MANAGEMENT

1. OVERVIEW

The objective is to obtain technical services to support and manage system security controls, authentication services, and role based software governing access to enterprise infrastructure and hosted systems, to support the National Information Technology Center (NITC), Security Division, Systems Security Branch.

2. SCOPE/DUTIES

The specific tasks to be supported and completed include, but are not limited to, those identified below.

a) The installation, administration, monitoring, operation, analysis, maintenance, and reporting of the enterprise authentication and authorization system (currently: Computer Associates, Identity Manager (IDM) Integrated with a Microsoft Active Directory (AD), Cisco Access Controls System, Quest Authentication Server and Entrust Token System).
b) The contractor shall organize, configure, and deploy the Microsoft Active Directory Forest, Domain, Organizational Units, Group Policy, Security Templates, and modify the LDAP protocol and LDAP attributes for hosted servers.
c) The contractor shall manage a Microsoft or Entrust Certificate Authority.
d) The contractor shall integrate a Role Based Access Controls (RBAC) process using Identity Management software with a Microsoft Active Directory.
e) The contractor shall work with mainframe system and network engineers to strengthen the security posture of enterprise systems using Authentication, Authorization, and Audit (AAA) and Public Key Infrastructure (PKI) services.
f) The contractor shall perform incident, problem, change, release, and configuration management following data center procedures.
g) The contractor shall work the service request ticket queues for access, accounts, roles, digital certificates, systems integration, and troubleshooting on hosted systems.
h) The contractor shall perform account management tasks on enterprise infrastructure and mainframe systems.
i) The contractor shall perform access control tasks on enterprise infrastructure and mainframe systems.
j) The contractor shall perform system, security, and application log and reports reviews following established procedures.
k) The contractor shall follow NITC's internal documented standards, processes, and procedures on Mid-Range and Mainframe platforms which govern user account management and system access controls.
l) The contractor shall document all aspects of the system for installation, daily operations, disaster recovery, and federal certification and accreditation requirements in the required format.
m) The contractor shall provide statistical reporting to illustrate enterprise security data.

n) The contractor shall follow NITC approved guidance from NIST.GOV Special Publications (Series: 800), USDA Departmental Directives (Series: 3100, 3300, 3400, 3500, 3600) and other applicable regulations and guidance for system controls in support of daily duties and audit requirements.
o) The contractor shall draft, review and submit security policy, standards, process, procedures, and system documentation.
p) The contractor shall support the technical evaluation and testing of security tools.
q) The contractor shall conduct security system and documentation reviews for managed systems.
r) The contractor shall analyze systems performance of new and existing equipment.
s) The contractor shall provide knowledge transfer to other team members, as well as to government personnel.

3. OTHER REQUIREMENTS

a) Mainframe platform experience is preferred.

4. ADDITIONAL INFORMATION AND REQUIREMENTS

The Government estimates that varying levels of requisite skill sets will be required to complete the stated requirements. The Government is providing the historical information below to illustrate the types of skill sets and the level-of-effort in terms of Full-Time-Equivalent (FTE) positions that have been utilized to support past requirements.

Number of FTE	General/Estimated Skill Level
4	intermediate
3	junior

CLIN 021 - SECURITY ADMINISTRATION SERVICES - MAINFRAME SECURITY, AUTHENTICATION, ROLE MANAGEMENT, AND ACCESS CONTROLS

1. OVERVIEW

The objective is to obtain security analysis and engineering services, including subject matter expert support, necessary for managing system security controls, authentication services, and role based software governing access to enterprise infrastructure and mainframe systems, in support of the Security Division, Systems Security Branch (SD/SSB) of the National Information Technology Center (NITC).

2. SCOPE/DUTIES

The specific tasks to be supported and completed include, but are not limited to, those identified below.

a) The administration, monitoring, operation, analysis, maintenance, and reporting of the mainframe authentication, authorization, and access controls system (currently: CA Access Control Facilities 2 (ACF2) and IBM Resource Access Control Facility (RACF)).
b) The contractor shall use Vanguard's VSS and the Eberhart Klemens Co. access rule clean up suite of tools to perform their access control tasks.
c) The contractor shall use the Computer Associates, CA Audit system and other supporting mainframe utilities for monitoring, diagnostics, and analysis.
d) The contractor shall execute native ACF2 / RACF commands utilizing GUI and panel-drive interfaces to administer ACF2 / RACF.
e) Establish and maintain ACF2 and RACF logon IDs.
f) Establish and maintain ACF2 and RACF security rules and parameters.
g) The contractor shall integrate a Role Based Access Controls (RBAC) process using Identity Management software.
h) The contractor shall work with mainframe system and network engineers to strengthen the security posture of enterprise systems using Authentication, Authorization, and Audit (AAA) and Public Key Infrastructure (PKI) services.
i) The contractor shall perform incident, problem, change, release, and configuration management following data center procedures.
j) The contractor shall work the service request ticket queues for access, accounts, roles, digital certificates, systems integration, and troubleshooting on hosted systems.
k) The contractor shall perform account management tasks on enterprise infrastructure and mainframe systems.
l) The contractor shall perform access control tasks on enterprise infrastructure and mainframe systems.
m) The contractor shall perform system, security, and application log and reports reviews following established procedures.
n) The contractor shall follow NITC's internal documented standards, processes, and procedures on Mid-Range and Mainframe platforms which govern user account management and system access controls.

o) The contractor shall document all aspects of the system for installation, daily operations, disaster recovery, and federal certification and accreditation requirements in the required format.
p) The contractor shall provide statistical reporting to illustrate enterprise security data.
q) The contractor shall follow NITC approved guidance from NIST.GOV Special Publications (Series: 800), USDA Departmental Directives (Series: 3100, 3300, 3400, 3500, 3600) and other applicable regulations and guidance for system controls in support of daily duties and audit requirements.
r) The contractor shall draft, review and submit security policy, standards, process, procedures, and system documentation.
s) The contractor shall support the technical evaluation and testing of security tools.
t) The contractor shall conduct security system and documentation reviews for managed systems.
u) The contractor shall analyze systems performance of new and existing equipment.
v) The contractor shall provide knowledge transfer to other team members, as well as to government personnel.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Recent experience (with in the last 12 months) on Mid-Range platform experience.
b) Experience with Active Directory / LDAP is preferred.
c) Experience with Identity Manager on the mainframe is preferred.
d) Experience as an application developer/programmer is preferred.

CLIN 022 - SECURITY ENGINEERING - ASSESSMENT SERVICES

1. OVERVIEW

The objective is to obtain technical support for security assessment tools, vulnerability scanning tools, and penetration testing to support the Security Division, Information Security Branch (SD/ISB). This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

a) Install, administer and manage the NITC vulnerability assessment environment.
b) Monitor Remedy ticket queues for the Information Security Branch (ISB) Assessment team and processes/works incidents and change request tickets as they are assigned to ISB Assessment.
c) Perform monthly and ad-hoc scans across the NITC network environment.
d) Document all aspects of the system for daily operations and disaster recovery, in addition to adherence of federal certification and accreditation requirements.
e) Provide statistical reporting to illustrate security posture and continuous improvements.
f) Participate in the creation, review and enforcement of security policy, procedures and system documentation.
g) Evaluate, make recommendations, implement or disseminate IT security tools, procedures and practices to protect organizational systems.
h) Provide knowledge transfer to team members, to include government counterparts.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Experience in networking design and concepts to include TCP/IP, switching, routing, firewalls, virtual route forwarding and VLANs.
b) Detailed experience and understanding of Microsoft, Linux and UNIX operating systems.
c) Experience in Information Security.
d) Experience with at least one of the following scanning technologies: eEye Retina, Rapid7 Nexpose, Metasploit, Core Impact, Nessus, dbProtect, or Appdetective.
e) Thorough understanding of the following security technologies:
   - Firewalls/Routers/Switches
   - Vulnerabilities/Risks/Threats
   - Cyber Incident Response techniques

CLIN 023 - SECURITY ENGINEERING – MONITORING, DETECTING AND ANALYSIS SERVICES

1. OVERVIEW

The objective is to obtain technical support for intrusion detection/prevention systems, security incident and event management (SIEM) tools, and other various network perimeter defense solutions, in support of the Security Division, Information Security Branch (SD/ISB). This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

a) Installs, administers and manages the NITC Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), Security Incident and Event Manager (SIEM), Wireless Intrusion Prevention Systems (WIPS) and Host-based Intrusion Detection systems (HIDS/HIPS).
b) Monitors Remedy ticket queues for Information Security Branch (ISB) Monitoring Detecting and Analyzing (MDA) team and processes/works incidents and change request tickets as they are assigned to ISB MDA.
c) Performs Incident Response activities by following the NITC Incident Response procedures in the event that a Cyber Incident occurs.
d) Documents all aspects of the system for daily operations and disaster recovery, in addition to adherence of federal certification and accreditation requirements.
e) Provides statistical reporting to illustrate security posture and continuous improvements.
f) Participates in the creation, review and enforcement of security policy, procedures and system documentation.
g) Evaluates, makes recommendations, implements or disseminates IT security tools, procedures and practices to protect organizational systems.
h) Provides knowledge transfer to team members, to include government counterparts.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Experience in networking design and concepts to include TCP/IP, switching, routing, firewalls, virtual route forwarding and VLANs.
b) Detailed experience and understanding of Microsoft, Linux and UNIX operating systems.
c) Experience with a Security Incident and Event Management (SIEM) tool.
d) Experience in Information Security.
e) Experience with one of the following IDS/IPS technologies: SourceFire, McAfee, HP TippingPoint, Cisco, and Snort.
f) Thorough understanding of the following security technologies:
   - Firewalls/Routers/Switches
   - Packet Capture (PCAP) analysis
   - IT System Forensics

CLIN 024 - SECURITY ENGINEERING - NETWORK ACCESS CONTROL SERVICES

1. OVERVIEW

The objective is to obtain technical support for firewalls, remote access solutions, and other various network perimeter defense solutions in support of the Security Division, Information Security Branch (SD/ISB) at the National Information Technology Center (NITC). This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

a) Installs, administers and manages the NITC firewalls, Access Control Lists (ACL), Virtual Private Network (VPN) systems and Web Proxies.
b) Monitors Remedy ticket queues for Information Security Branch (ISB) Network Access Control (NAC) team and processes/works incidents and change request tickets as they are assigned to ISB NAC.
c) Documents all aspects of the system for daily operations and disaster recovery, in addition to adherence of federal certification and accreditation requirements.
d) Provides statistical reporting to illustrate security posture and continuous improvements.
e) Participates in the creation, review and enforcement of security policy, procedures and system documentation.
f) Evaluates, makes recommendations, implements or disseminates IT security tools, procedures and practices to protect organizational systems.
g) Provides knowledge transfer to team members, to include government counterparts.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS:

a) Experience in networking design and concepts to include TCP/IP, switching, routing, firewalls, virtual route forwarding and VLANs.
b) Experience in Information Security.
c) Experience with two of the following firewall technologies: Juniper/Netscreen, Cisco, Checkpoint, Fortinet, Palo Alto.
d) Thorough understanding of the following security technologies:
   - Intrusion Detection/Prevention Systems (IDS/IPS)
   - Log Management and Security Incident and Event Management (SIEM)
   - Virtual Private Network (VPN) Remote Access
   - Web Content Filtering / Web Proxy

CLIN 025 - SENIOR APPLICATIONS ENGINEERING SERVICES

1. OVERVIEW

The objective is to obtain technical support services required to execute the transition of USDA and non-USDA customer business applications to the USDA Enterprise Data Centers (EDC).

In 2010, the Office of Management and Budget initiated the Federal Data Center Consolidation Initiative (FDCCI). The focus of the FDCCI is to reduce the number of computer rooms, the amount of energy consumption, and to consolidate business applications into designated Agency EDCs.

The contractor will be required to focus on transitioning business applications and will be the primary NITC point-of-contact between the customer and applicable EDC representatives. The contractor will be required to make contact with NITC customers, technical staff, business partners, management, and internal and external auditors.

2. SCOPE/DUTIES

The specific tasks to be supported by the contractor include, but are not limited to, those listed below.

a) The contractor shall complete all task activities in accordance with NITC service offerings, tools, and best practices.
b) Meet with customers as required to gain a sufficient understanding of their business application environment (e.g., critical application production timeframes).
c) Develop .customer application inventories to capture operating systems, application languages, databases, storage protocols and volume, customer and administrator access methods, application architecture, and application interdependencies.
d) Utilize NITC server and desktop discovery tools and resulting information to assist in the development of EDC hosting estimates
e) Utilize NITC server and desktop discovery tools and resulting information to develop EDC target architectures.
f) Gain an understanding of customer application test plans and assist in test plan execution.
g) Ensure customer access requirements to application target architecture are operational and meet customer requirements.
h) Execute, directly with customer, application test plans and maintain primary point-of-contact role between customer and applicable EDC representatives to minimize issue resolution timeframes.
i) Ensure that customer test plans are successful, resolve related issues, and coordinate with EDC Engineers on any final application architecture changes.
j) Provide continued support to ensure customer application transitions are successfully completed.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Well-rounded skills in networking, security, storage solutions, disaster recovery as well as a more detailed skill set in working with operating systems, applications and databases.
b) Implementing Open Systems Interconnection model architecture which includes routing, switching, VLANs, load balancing and traffic analysis.
c) Security – firewall, access controls, Active Directory and application vulnerability scanning.
d) Storage – Storage Area Network, Network Attached Storage, large data transfers and back-up/recovery.
e) Disaster Recovery Strategies – Active-Active and Active-Passive.
f) Operating Systems – Windows, Linux, AIX, HP-UX, Solaris and virtualization technologies.
g) Applications and Database – Application design and architecture in n-tier environments. Migration of applications utilizing server and desktop discovery tools and develop/execute application test plans. Required application environments and databases are, but not limited to, J2EE, .NET, IIS, Apache, Oracle, MS SQL and DB2

CLIN 026 - SERVER AUTOMATION TOOL SUPPORT SERVICES

1. OVERVIEW

The objective is to obtain Server Automation Tool Support Services for Open Systems (UNIX) and Microsoft (WINDOWS SERVER) computing platforms at the National Information Technology Center (NITC). The NITC currently utilizes BMC Server Automation, BMC Orchestrator, and BMC Advanced Reporter. The Microsoft and Open systems platforms will be referenced as "midrange" in the remainder of this document**.**

2. SCOPE/DUTIES

The Contractor shall provide Server Automation Tool Support Services support for NITC. The specific tasks to be supported and completed include, but are not limited to, those identified below.

a) Install, test, configure, customize, and maintain the server automation tools. This includes upgrades as well as agents on servers.
b) Create, schedule, perform, maintain and monitor server automation jobs.
c) Support patching requirements as required.
d) Support the automation of system provisioning
e) Create, execute, troubleshoot, and maintain optimized automation scripts.
f) Develop, execute and maintain standard and custom reports for ongoing metrics and data calls.
g) Collaborate with BMC Remedy, Atrium Discovery and Dependency Mapping (ADDM), Atrium Configuration Management Database (CMDB), and BMC ProactiveNet Performance Monitoring (BPPM) teams to support integration efforts using BMC Orchestrator.
h) Create, execute, troubleshoot, and maintain optimized custom scripts for managing security compliance.
i) Perform hardening of systems per NITC, OCIO Cyber-Security, and Departmental Policies, Standards, Regulations, and Notices, to include security monitoring and updating of certification/accreditation procedures.
j) Confirm that server automation environment is backed up as required and ensure disaster recovery readiness.
k) Make recommendations for server automation system performance improvements.
l) Troubleshoot overall system problems and identify/resolve problems.
m) Manage the role-based access control (RBAC) security model of NITC and customer access into the server automation console.
n) Document and perform changes and resolve incidents and problems using NITC's Configuration Management Tools and Systems.

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Recent (within the last 12 months) experience with BMC Server Automation and Orchestrator required, including installation, configuration, operation, upgrading, and providing maintenance of the product.
b) Systems administration techniques on IBM AIX, Microsoft Windows Server, Oracle Solaris, and RedHat Linux operating systems, operating in a complex, diverse, enterprise environment, is preferred.
c) Virtualization techniques such as IBM LPARs, Solaris Zones, and VMware hypervisor, is preferred.

CLIN 027 - STORAGE ADMINISTRATION SERVICES

1. OVERVIEW

The objective is to obtain technical support for storage administration assistance to the Information Services Division, Storage Management Branch (ISD/SMB), National Information Technology Center (NITC). The contractor shall perform various duties, particularly in the technical areas of Storage Area Network (SAN) administration, Network Attached Storage (NAS) administration, Cloud Storage, Software-Defined Storage (SDS), Virtual Tape administration, and Open Systems Backup administration.

This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors. Contractor shall follow SMB hardening guides and storage procedures.

2. SCOPE/DUTIES

The SMB currently operates storage environments in six data centers (Kansas City, MO; Beltsville, MD; St Louis, MO; Fort Collins, CO; Fort Worth, TX; and Salt Lake City, UT). Storage administration duties shall be performed remotely for Beltsville MD. The storage solutions operated by NITC are based on Brocade switch technology, Hitachi Data Systems (HDS) enterprise disk technology, SUN/StorageTek (STK) enterprise tape technology, Symantec NetBackup software, EMC Data Domain, and EMC enterprise and modular disk technology (with a few sites having SUN disk technology for archiving), NetApp appliances, Ceph for cloud storage, and IBM Virtual Tape System for mainframe.

All required services are to be provided by the contractor and shall comply with applicable standards, policies, and procedures. The Contractor shall implement security controls, create/update documentation, to include configuration and automated processes, and develop project plans/tasks lists. Categories of services to be provided include, but are not limited to, the following:

- Storage administration services
- Storage design and architecture
- Storage virtualization
- Storage maintenance
- Storage performance evaluation and analysis

Specific tasks include, but are not limited to, those identified in the subsequent paragraphs.

a) Installing and configuring software; completing backup and restore requests; performing storage allocations; adding clients to backup policies; decommissioning systems; configuring media and master servers/drives/robots; performing updates/upgrades/patches to hardware/software/firmware; troubleshooting issues; monitoring systems; and reporting, etc.

b) Development and maintenance of required documentation. The documentation includes, but is not limited to, the following: SAN Billing Table, configuration documents, NetBackup documents, SAN administration request form, etc.
c) Operation of all aspects of storage administration tools and products including installation, configuration, operation, upgrading, and providing maintenance of products.
d) Scheduling, building, troubleshooting automation jobs, including compliance and remediation jobs, auditing jobs, package installation, and provisioning jobs.
e) Installing, configuring, upgrading, maintaining, and creating reports using reporting tools.
f) Monitoring and recommending improvements for performance of storage products.
g) The contractor shall perform the following frequently recurring project tasks and special projects that incorporate the duties described above.
   - Disk Storage administration and support – Occurs daily
   - SAN Switch administration and support – Occurs daily
   - NAS Solution administration and support – Occurs daily
   - Tape Storage administration and support – Occurs daily
   - Symantec NetBackup administration and support – Occurs daily
   - Oral and written communication with NITC management as well as internal and external customers – Occurs daily
   - Disaster Recovery Testing Activities – As required, approximately 1-2 times per month
   - Disaster Recovery Planning and Documentation – As required.
   - NITC Vital Records Documentation – As required unless specifically assigned documentation tasks, then daily.
   - Weekly Activity Reporting – Occurs weekly
   - Configuration Management and Change Control Procedures – As required, approximately 1-2 times per week, includes specific storage documents

3. EXPERIENCE AND EXPERTISE REQUIREMENTS

The contractor shall have the following general experience and expertise:

- Specialized experience with enterprise storage solutions.
- Experience with storage administration techniques on enterprise class storage, mid-tier storage, and direct attached storage.
- Familiar with virtualization techniques such as IBM LPARs, Solaris Zones, and VMware.
- Familiar with requirements for telecommunication.

The contractor shall have the following specific experience and expertise:

- SAN Disk Technologies:
  - HDS enterprise disk technology (e.g. 9980, USP, USP-V, VSP and etc.) provisioning and performance management in a SAN storage environment.
  - Remote and In-System Replication configuration and support.
  - Hitachi Universal Replicator (HUR), and subsystem architecture and configuration.
  - IBM (DS8000), EMC (DMX, Data Domain, and Clariion), and other industry leading disk technologies.
  - Working knowledge of EMC ECC.

- Installation and upgrade the ECC console.
- Utilization of Performance Monitor and in depth analysis of EMC devices.
- Working knowledge of EMC replication software, SRDF.
- Working knowledge of setup and administration of mirror pairs between remote sites.

- Cloud Technologies:
  - Cloud storage technologies such as Ceph to manage vast amounts of data and applications with different storage interface needs.
  - Knowledgeable of Ceph's Reliable Autonomic Distributed Object Store (RADOS).

- SDS Technologies:
  - Implementation and management of software-defined storage solutions to support dynamic applications and workloads in virtualized environments.

- SAN Switch Technologies:
  - Brocade SAN switch technology operation, provisioning, and support.
  - Familiar with SAN channel extension technologies used for remote data replication purposes.

- SAN Tape Technologies:
  - SUN/STK automated tape technologies (e.g. 9310, L700, SL8500, etc.).
  - STK Automated Cartridge System Library Software (ACSLS).
  - 9840 and LTO tape drive technology.
  - SUN Storage Archive Manager File System (SAMFS) archive solution.

- NAS Technologies:
  - NetApp Appliance technology (e.g. 6200, 3020, v3140, etc.)
  - vFilers
  - Common Internet File System (CIFS)
  - Network File System (NFS)

- Virtual Tape Technologies:
  - Virtual Tape technology (e.g. Data Domain Appliances for Open Systems and IBM Virtual Tape System (VTS) for mainframe), including HUR, NetBackup, and/or VTS Grid.

- Open Systems Backup Technologies:
  - Symantec NetBackup installation, administration, maintenance, and support in an enterprise environment including Microsoft Windows, Sun Solaris, and IBM AIX clients and media servers.

- Backup and Archive Technologies:
  - SAMFS installation, administration, maintenance, and support in an enterprise environment.